PCI DSS Scan Report Executive Summary

Exhibit 10R

sysnet global solutions Powered by Qualys.

PCI DSS Scan Report Executive Summary

A.1 Scan Customer Information				A.2 Approved Scanning Vendor Information			
Company:	G0007 PLANET FITNESS BRICK			Company:	Sysnet		
Contact:	Ryan Wagner	Title:		Contact:	gopi balachenna	Title:	ASV
Telephone:		Email:	ryan.wagner@pfgrwth.com	Telephone:	+35314951300	Email:	balachenna.gopi@sysnetgs.com
Business address:	5425 BALTIMORE NTL PIKE BALTIMORE Maryland			Business address:	4th Floor The Herbert Building Carrickmines Dublin 18 Republic Of Ireland		
URL:				URL:	www.sysnetglobalsolutions.com		
MID:	ABC0325						
Other Mids covered by this scan result	ABC0708 ABC9308 ABC9232 ABC0695 ABC8091 ABC9318 ABC9120 ABC9260 ABC1763 ABC7086 ABC8076 ABC7211 ABC7606 ABC93311 ABC6063 ABC8127 ABC0469 ABC0929 ABC0786 ABC6415 ABC4185 ABC0706 ABC0838 ABC7903 ABC9408 ABC0906 ABC9351 ABC0585 ABC0711 ABC0914 ABC5263 ABC9678 ABC6025 ABC8105 ABC9362 ABC8334 ABC0877 ABC7035						

Exhibit 10R

A.1 Scan Customer Information	A.2 Approved Scanning Vendor Information
ABC3555	
ABC7483	
ABC9165	
ABC8146	
ABC0710	
ABC6905	
ABC0669	
ABC0907	
ABC1279	
ABC0263	
ABC0709	
ABC0177	
ABC9539	
ABC6523	
ABC0787	
ABC0888	
ABC0963	
ABC2837	
ABC8702	
ABC9358	
ABC93088	
ABC0625	
ABC0705	
ABC0707	
ABC6342	
ABC0503	
ABC7085	
ABC8884	
ABC2738	
ABC0349	
ABC8585	
ABC9363	
ABC2523	
ABC7246	

Exhibit 10R

A.3 Scan status

Date scan completed	July 14, 2022	Scan expiration date (90 days from date scan completed)	October 12, 2022
Compliance status:	PASS	Scan report type	Full Scan
Number of unique in-scope components[4] scanned			68
Number of identified failing vulnerabilities			0
Number of components found by ASV but not scanned because scan customer confirmed components were out of scope			0

[4] A Components includes any host, virtual host, IP address, FQDN or unique vector into a system or cardholder data environment.

PCI DSS Scan Report Executive Summary

Exhibit 10R

sysnet. global solutions Powered by Qualys.

A.1 Scan Customer Information				A.2 Approved Scanning Vendor Information			
Company:	G0007 PLANET FITNESS BRICK			Company:	Sysnet		
Contact:	Ryan Wagner	Title:		Contact:	gopi balachenna	Title:	ASV
Telephone:		Email:	ryan.wagner@pfgrwth.com	Telephone:	+35314951300	Email:	balachenna.gopi@sysnetgs.com
Business address:	5425 BALTIMORE NTL PIKE BALTIMORE Maryland			Business address:	4th Floor The Herbert Building Carrickmines Dublin 18 Republic Of Ireland		
URL:				URL:	www.sysnetglobalsolutions.com		
MID:	ABC0325						
Other Mids covered by this scan result	ABC7085						
	ABC0707						
	ABC0711						
	ABC9351						
	ABC0709						
	ABC9363						
	ABC93088						
	ABC0263						
	ABC8127						
	ABC0710						
	ABC9260						
	ABC2738						
	ABC0625						
	ABC9308						
	ABC8105						
	ABC0786						
	ABC0929						
	ABC8091						
	ABC6415						
	ABC0838						
	ABC0877						
	ABC7086						
	ABC8146						
	ABC9408						
	ABC7903						
	ABC9232						
	ABC6025						
	ABC9165						
	ABC0914						
	ABC0669						
	ABC8334						
	ABC9539						
	ABC0888						
	ABC1279						
	ABC0706						
	ABC0469						
	ABC6342						
	ABC7483						

Exhibit 10R

A.1 Scan Customer Information

ABC7035
ABC6523
ABC6063
ABC3555
ABC9318
ABC0349
ABC7211
ABC93311
ABC0906
ABC8076
ABC0787
ABC4185
ABC9362
ABC0705
ABC8585
ABC2837
ABC8702
ABC6905
ABC7606
ABC0708
ABC2523
ABC7246
ABC0585
ABC1763
ABC5263
ABC0963
ABC0503
ABC0177
ABC9678
ABC0907
ABC9358
ABC9120
ABC8884
ABC0695

A.2 Approved Scanning Vendor Information

Exhibit 10R

A.3 Scan status

Date scan completed	September 01, 2022	Scan expiration date (90 days from date scan completed)	November 30, 2022
Compliance status:	PASS	Scan report type	Full Scan
Number of unique in-scope components[4] scanned			70
Number of identified failing vulnerabilities			0
Number of components found by ASV but not scanned because scan customer confirmed components were out of scope			0

[4] A Components includes any host, virtual host, IP address, FQDN or unique vector into a system or cardholder data environment.

PCI DSS Scan Report Executive Summary

Exhibit 10R

sysnet global solutions Powered by Qualys.

A.1 Scan Customer Information

Company:	G0007 PLANET FITNESS BRICK		
Contact:	Ryan Wagner	Title:	
Telephone:		Email:	ryan.wagner@pfgrwth.com
Business address:	5425 BALTIMORE NTL PIKE BALTIMORE Maryland		
URL:			
MID:	ABC0325		
Other Mids covered by this scan result	ABC93088 ABC9260 ABC93311 ABC0349 ABC8105 ABC0787 ABC0669 ABC2837 ABC1763 ABC7211 ABC0963 ABC9232 ABC0786 ABC7483 ABC9539 ABC0907 ABC0709 ABC9165 ABC8702 ABC9351 ABC9318 ABC7606 ABC2738 ABC8585 ABC8091 ABC9363 ABC9362 ABC0906 ABC7085 ABC8884 ABC0711 ABC0929 ABC7246 ABC2523 ABC6025 ABC0710 ABC0838 ABC7035		

A.2 Approved Scanning Vendor Information

Company:	Sysnet		
Contact:	gopi balachenna	Title:	ASV
Telephone:	+35314951300	Email:	balachenna.gopi@sysnetgs.com
Business address:	4th Floor The Herbert Building Carrickmines Dublin 18 Republic Of Ireland		
URL:	www.sysnetglobalsolutions.com		

Exhibit 10R

A.1 Scan Customer Information	A.2 Approved Scanning Vendor Information
ABC9120	
ABC0263	
ABC0708	
ABC0914	
ABC0503	
ABC0705	
ABC0695	
ABC7903	
ABC4185	
ABC9308	
ABC8076	
ABC8127	
ABC0877	
ABC0585	
ABC0706	
ABC9678	
ABC9408	
ABC9358	
ABC7086	
ABC0469	
ABC6415	
ABC6342	
ABC0888	
ABC8146	
ABC3555	
ABC6905	
ABC8334	
ABC0625	
ABC0707	
ABC5263	
ABC6523	
ABC0177	
ABC1279	
ABC6063	

Exhibit 10R

A.3 Scan status

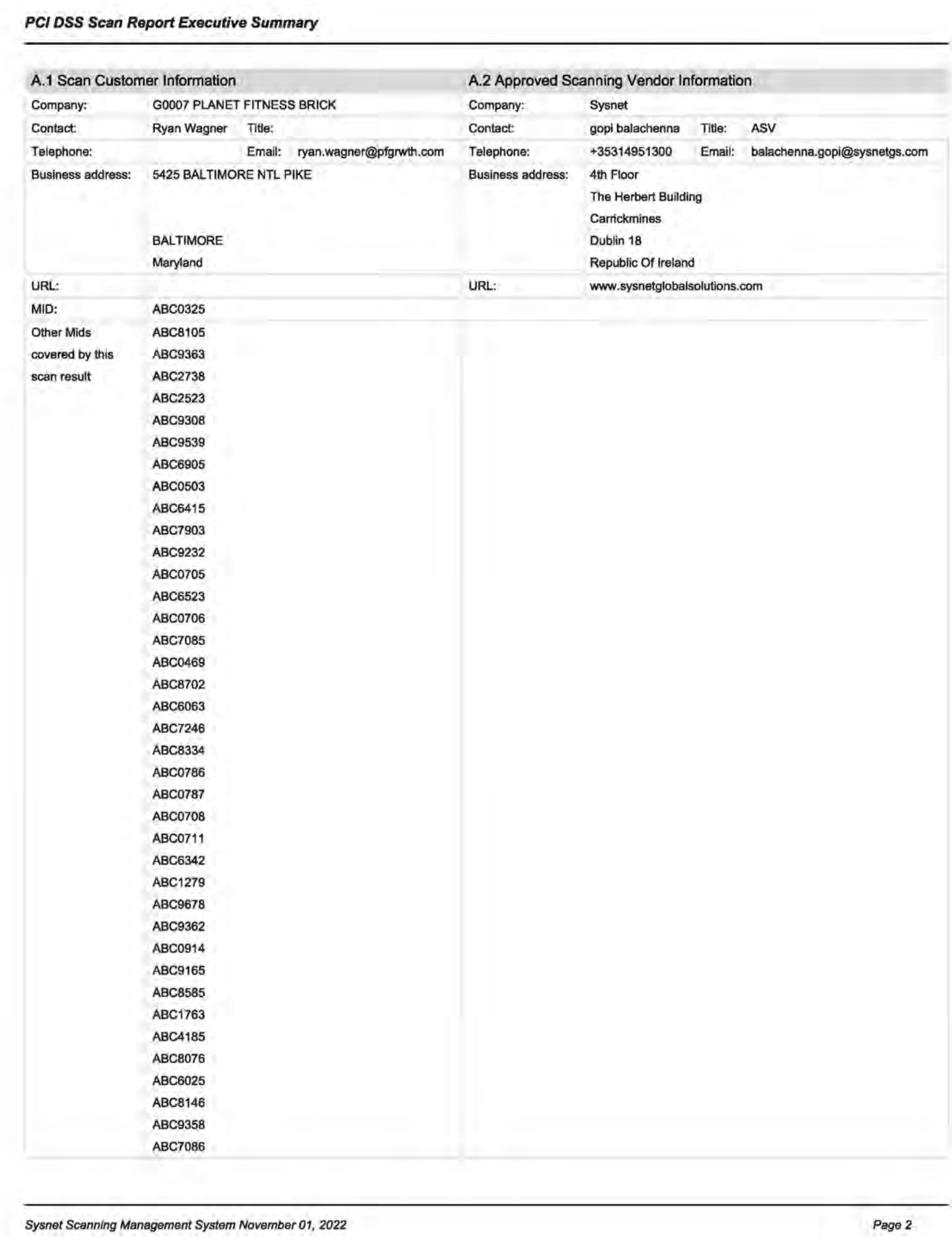
Date scan completed	October 01, 2022	Scan expiration date (90 days from date scan completed)	December 30, 2022
Compliance status:	PASS	Scan report type	Full Scan
Number of unique in-scope components[4] scanned			69
Number of identified failing vulnerabilities			0
Number of components found by ASV but not scanned because scan customer confirmed components were out of scope			0

[4] A Components includes any host, virtual host, IP address, FQDN or unique vector into a system or cardholder data environment.

PCI DSS Scan Report Executive Summary

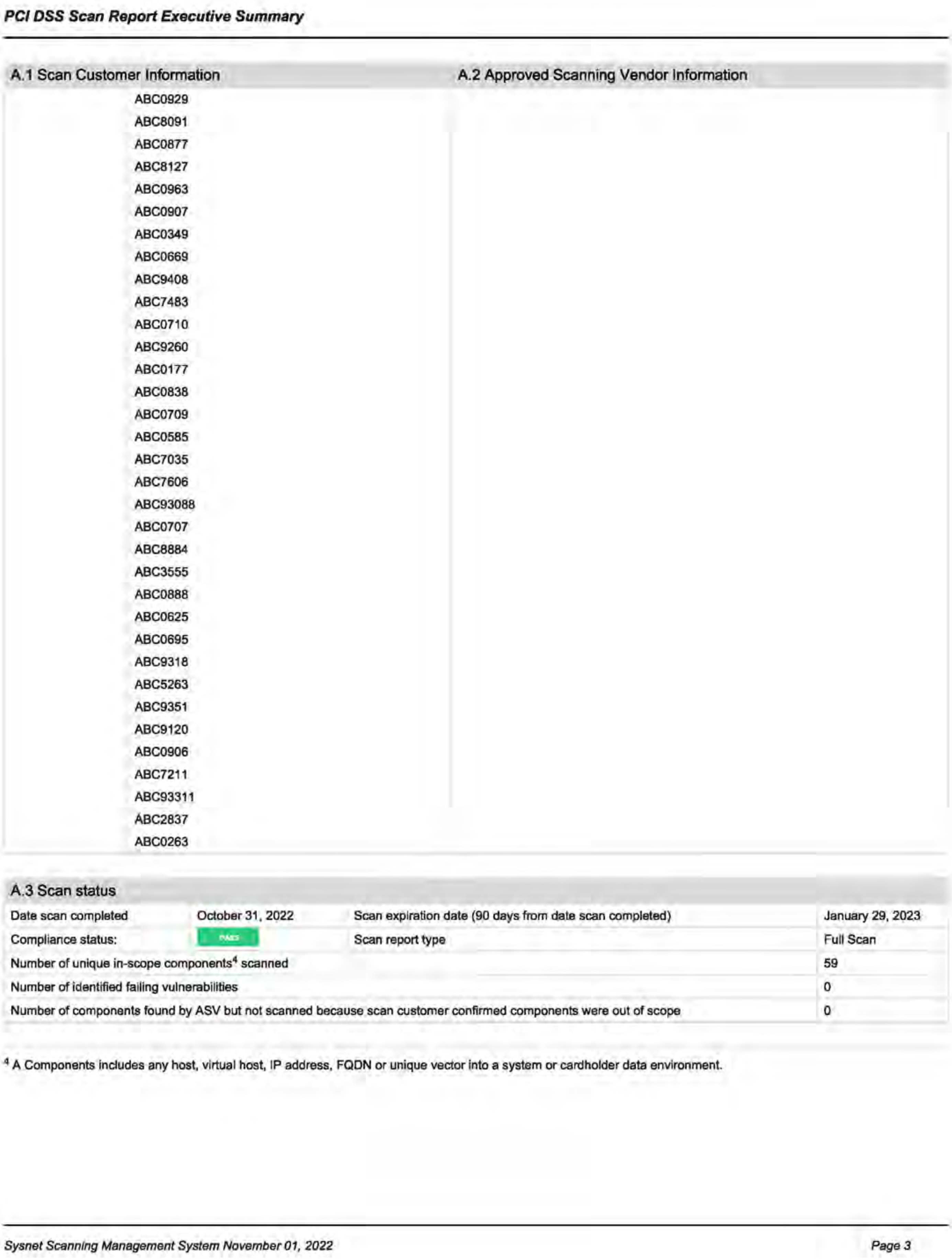
Exhibit 10R

sysnet global solutions Powered by Qualys.



A.1 Scan Customer Information				A.2 Approved Scanning Vendor Information			
Company:	G0007 PLANET FITNESS BRICK			Company:	Sysnet		
Contact:	Ryan Wagner	Title:		Contact:	gopi balachenna	Title:	ASV
Telephone:		Email:	ryan.wagner@pfgrwth.com	Telephone:	+35314951300	Email:	balachenna.gopi@sysnetgs.com
Business address:	5425 BALTIMORE NTL PIKE BALTIMORE Maryland			Business address:	4th Floor The Herbert Building Carrickmines Dublin 18 Republic Of Ireland		
URL:				URL:	www.sysnetglobalsolutions.com		
MID:	ABC0325						
Other Mids covered by this scan result	ABC8105 ABC9363 ABC2738 ABC2523 ABC9308 ABC9539 ABC6905 ABC0503 ABC6415 ABC7903 ABC9232 ABC0705 ABC6523 ABC0706 ABC7085 ABC0469 ABC8702 ABC6063 ABC7246 ABC8334 ABC0786 ABC0787 ABC0708 ABC0711 ABC6342 ABC1279 ABC9678 ABC9362 ABC0914 ABC9165 ABC8585 ABC1763 ABC4185 ABC8076 ABC6025 ABC8146 ABC9358 ABC7086						

Exhibit 10R



A.1 Scan Customer Information

ABC0929
ABC8091
ABC0877
ABC8127
ABC0963
ABC0907
ABC0349
ABC0669
ABC9408
ABC7483
ABC0710
ABC9260
ABC0177
ABC0838
ABC0709
ABC0585
ABC7035
ABC7606
ABC93088
ABC0707
ABC8884
ABC3555
ABC0888
ABC0625
ABC0695
ABC9318
ABC5263
ABC9351
ABC9120
ABC0906
ABC7211
ABC93311
ABC2837
ABC0263

A.2 Approved Scanning Vendor Information

A.3 Scan status

Date scan completed	October 31, 2022	Scan expiration date (90 days from date scan completed)	January 29, 2023
Compliance status:	🟩 PASS	Scan report type	Full Scan
Number of unique in-scope components[4] scanned			59
Number of identified failing vulnerabilities			0
Number of components found by ASV but not scanned because scan customer confirmed components were out of scope			0

[4] A Components includes any host, virtual host, IP address, FQDN or unique vector into a system or cardholder data environment.

Exhibit 10R

PCI DSS Scan Report Executive Summary

Exhibit 10R

sysnet. global solutions Powered by Qualys.

A.1 Scan Customer Information

Company:	G0007 PLANET FITNESS BRICK		
Contact:	Ryan Wagner	Title:	
Telephone:		Email:	ryan.wagner@pfgrwth.com
Business address:	5425 BALTIMORE NTL PIKE BALTIMORE Maryland		
URL:			
MID:	ABC0325		
Other Mids covered by this scan result	ABC8334 ABC9539 ABC0705 ABC0786 ABC8702 ABC0711 ABC7606 ABC8091 ABC8076 ABC6342 ABC6025 ABC7246 ABC0585 ABC0625 ABC6063 ABC9362 ABC9232 ABC2523 ABC0963 ABC7903 ABC0469 ABC9308 ABC0707 ABC9260 ABC0177 ABC0669 ABC0706 ABC0263 ABC0349 ABC6523 ABC0906 ABC2837 ABC93311 ABC0907 ABC7085 ABC9120 ABC9165 ABC0503		

A.2 Approved Scanning Vendor Information

Company:	Sysnet		
Contact:	gopi balachenna	Title:	ASV
Telephone:	+35314951300	Email:	balachenna.gopi@sysnetgs.com
Business address:	4th Floor The Herbert Building Carrickmines Dublin 18 Republic Of Ireland		
URL:	www.sysnetglobalsolutions.com		

Exhibit 10R

A.1 Scan Customer Information

ABC0695
ABC8105
ABC1763
ABC5263
ABC0709
ABC9358
ABC3555
ABC0914
ABC7483
ABC0877
ABC8884
ABC9351
ABC0787
ABC6415
ABC0888
ABC8127
ABC9408
ABC0838
ABC2738
ABC7035
ABC93088
ABC4185
ABC8146
ABC6905
ABC0929
ABC7086
ABC0708
ABC9363
ABC1279
ABC7211
ABC8585
ABC9678
ABC0710
ABC9318

A.2 Approved Scanning Vendor Information

A.3 Scan status

Date scan completed	December 01, 2022	Scan expiration date (90 days from date scan completed)	March 01, 2023
Compliance status:	PASS	Scan report type	Full Scan
Number of unique in-scope components[4] scanned			45
Number of identified failing vulnerabilities			0
Number of components found by ASV but not scanned because scan customer confirmed components were out of scope			0

[4] A Components includes any host, virtual host, IP address, FQDN or unique vector into a system or cardholder data environment.

Exhibit 10R

PCI DSS Scan Report Executive Summary

Exhibit 10R

sysnet global solutions Powered by Qualys.

A.1 Scan Customer Information

Company:	G0007 PLANET FITNESS BRICK		
Contact:	CieloIT Support	Title:	
Telephone:		Email:	support@cieloit.com
Business address:	5425 BALTIMORE NTL PIKE BALTIMORE Maryland		
URL:			
MID:	ABC0325		
Other Mids covered by this scan result	ABC7035		
	ABC7086		
	ABC7246		
	ABC7211		
	ABC1763		
	ABC0888		
	ABC8334		
	ABC8585		
	ABC9363		
	ABC0669		
	ABC0263		
	ABC9308		
	ABC8146		
	ABC0710		
	ABC6025		
	ABC8105		
	ABC93311		
	ABC0838		
	ABC1279		
	ABC6342		
	ABC8884		
	ABC6415		
	ABC0906		
	ABC0929		
	ABC0708		
	ABC7085		
	ABC6905		
	ABC6063		
	ABC0907		
	ABC0786		
	ABC6523		
	ABC5263		
	ABC0914		
	ABC2837		
	ABC0877		
	ABC9260		
	ABC0177		
	ABC0963		

A.2 Approved Scanning Vendor Information

Company:	Sysnet		
Contact:	gopi balachenna	Title:	ASV
Telephone:	+35314951300	Email:	balachenna.gopi@sysnetgs.com
Business address:	4th Floor The Herbert Building Carrickmines Dublin 18 Republic Of Ireland		
URL:	www.sysnetglobalsolutions.com		

Exhibit 10R

A.1 Scan Customer Information	A.2 Approved Scanning Vendor Information
ABC8127	
ABC0709	
ABC7483	
ABC0705	
ABC0787	
ABC3555	
ABC0585	
ABC0469	
ABC9120	
ABC9678	
ABC9232	
ABC9351	
ABC0625	
ABC0707	
ABC7606	
ABC2738	
ABC8091	
ABC9318	
ABC0349	
ABC4185	
ABC93088	
ABC0695	
ABC2523	
ABC8702	
ABC0503	
ABC9408	
ABC0711	
ABC7903	
ABC0706	
ABC8076	
ABC9362	
ABC9165	
ABC9358	
ABC9539	

A.3 Scan status

Date scan completed	March 08, 2023	Scan expiration date (90 days from date scan completed)	June 06, 2023
Compliance status:	PASS	Scan report type	Full Scan
Number of unique in-scope components[4] scanned			73
Number of identified failing vulnerabilities			0
Number of components found by ASV but not scanned because scan customer confirmed components were out of scope			0

[4] A Components includes any host, virtual host, IP address, FQDN or unique vector into a system or cardholder data environment.

Exhibit 10R

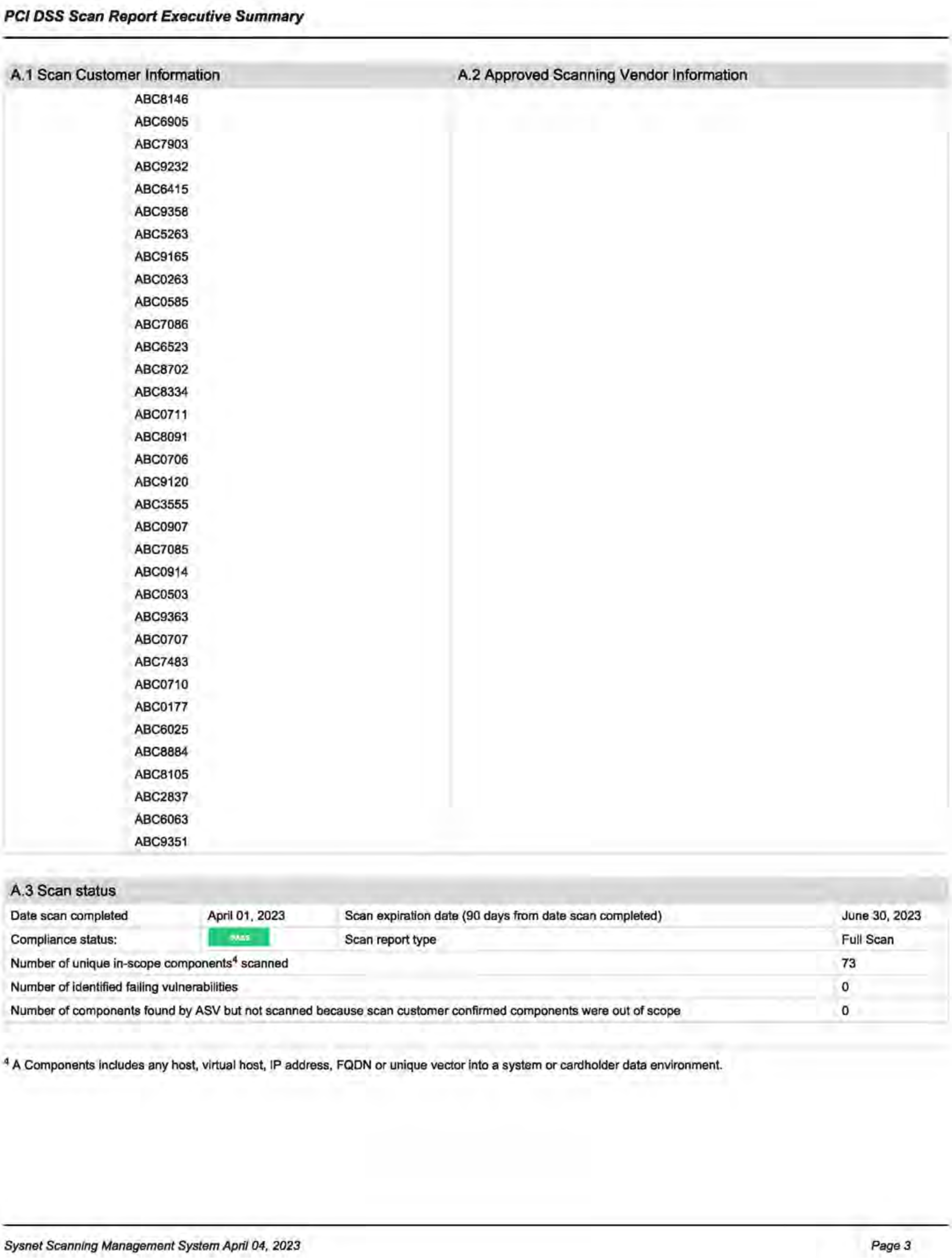
PCI DSS Scan Report Executive Summary

Exhibit 10R

sysnet global solutions Powered by Qualys.

A.1 Scan Customer Information		A.2 Approved Scanning Vendor Information	
Company:	G0007 PLANET FITNESS BRICK	Company:	Sysnet
Contact:	Ryan Wagner Title:	Contact:	gopi balachenna Title: ASV
Telephone:	Email: ryan.wagner@pfgrwth.com	Telephone:	+35314951300 Email: balachenna.gopi@sysnetgs.com
Business address:	5425 BALTIMORE NTL PIKE BALTIMORE Maryland	Business address:	4th Floor The Herbert Building Carrickmines Dublin 18 Republic Of Ireland
URL:		URL:	www.sysnetglobalsolutions.com
MID:	ABC0325		
Other Mids covered by this scan result	ABC1763 ABC9539 ABC1279 ABC0708 ABC2738 ABC0906 ABC7606 ABC6342 ABC8127 ABC7246 ABC0469 ABC0625 ABC7211 ABC9678 ABC9408 ABC0669 ABC0787 ABC8076 ABC93088 ABC9318 ABC0929 ABC93311 ABC2523 ABC0695 ABC0877 ABC0705 ABC4185 ABC0709 ABC0963 ABC0888 ABC9308 ABC0349 ABC0838 ABC9260 ABC8585 ABC7035 ABC9362 ABC0786		

Exhibit 10R



A.1 Scan Customer Information	A.2 Approved Scanning Vendor Information
ABC8146	
ABC6905	
ABC7903	
ABC9232	
ABC6415	
ABC9358	
ABC5263	
ABC9165	
ABC0263	
ABC0585	
ABC7086	
ABC6523	
ABC8702	
ABC8334	
ABC0711	
ABC8091	
ABC0706	
ABC9120	
ABC3555	
ABC0907	
ABC7085	
ABC0914	
ABC0503	
ABC9363	
ABC0707	
ABC7483	
ABC0710	
ABC0177	
ABC6025	
ABC8884	
ABC8105	
ABC2837	
ABC6063	
ABC9351	

A.3 Scan status

Date scan completed	April 01, 2023	Scan expiration date (90 days from date scan completed)	June 30, 2023
Compliance status:	PASS	Scan report type	Full Scan
Number of unique in-scope components[4] scanned			73
Number of identified failing vulnerabilities			0
Number of components found by ASV but not scanned because scan customer confirmed components were out of scope			0

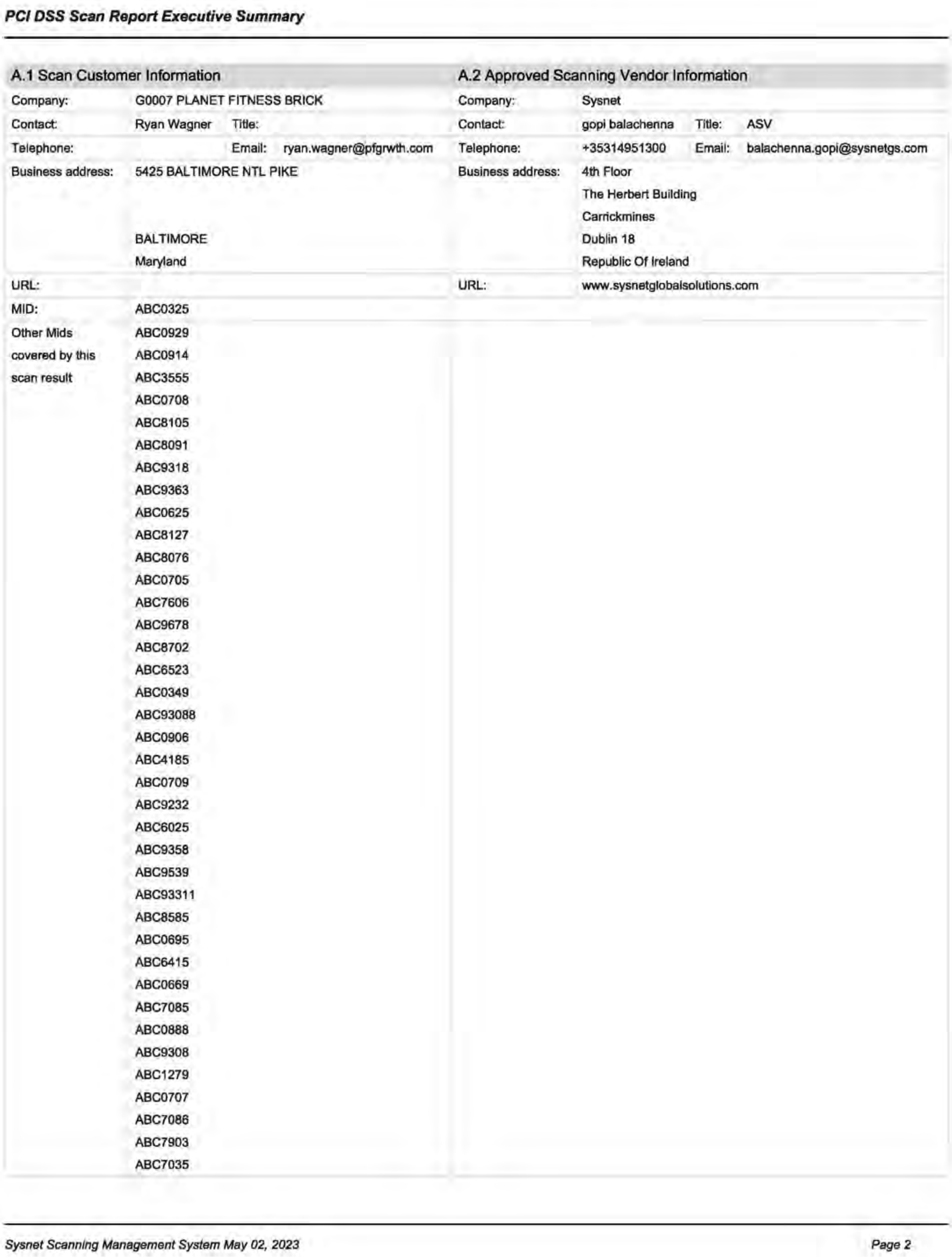
[4] A Components includes any host, virtual host, IP address, FQDN or unique vector into a system or cardholder data environment.

Exhibit 10R

PCI DSS Scan Report Executive Summary

Exhibit 10R

sysnet. global solutions Powered by Qualys.



A.1 Scan Customer Information				A.2 Approved Scanning Vendor Information			
Company:	G0007 PLANET FITNESS BRICK			Company:	Sysnet		
Contact:	Ryan Wagner	Title:		Contact:	gopi balachenna	Title:	ASV
Telephone:		Email:	ryan.wagner@pfgrwth.com	Telephone:	+35314951300	Email:	balachenna.gopi@sysnetgs.com
Business address:	5425 BALTIMORE NTL PIKE BALTIMORE Maryland			Business address:	4th Floor The Herbert Building Carrickmines Dublin 18 Republic Of Ireland		
URL:				URL:	www.sysnetglobalsolutions.com		
MID:	ABC0325						
Other Mids covered by this scan result	ABC0929 ABC0914 ABC3555 ABC0708 ABC8105 ABC8091 ABC9318 ABC9363 ABC0625 ABC8127 ABC8076 ABC0705 ABC7606 ABC9678 ABC8702 ABC6523 ABC0349 ABC93088 ABC0906 ABC4185 ABC0709 ABC9232 ABC6025 ABC9358 ABC9539 ABC93311 ABC8585 ABC0695 ABC6415 ABC0669 ABC7085 ABC0888 ABC9308 ABC1279 ABC0707 ABC7086 ABC7903 ABC7035						

Exhibit 10R

A.1 Scan Customer Information

ABC6905
ABC0710
ABC0263
ABC1763
ABC2837
ABC8334
ABC8884
ABC6063
ABC0786
ABC0963
ABC9362
ABC5263
ABC8146
ABC0877
ABC9165
ABC0585
ABC9408
ABC6342
ABC2523
ABC0907
ABC0503
ABC7211
ABC0177
ABC0469
ABC7246
ABC0711
ABC0787
ABC9351
ABC7483
ABC2738
ABC9260
ABC9120
ABC0706
ABC0838

A.2 Approved Scanning Vendor Information

A.3 Scan status

Date scan completed	May 01, 2023	Scan expiration date (90 days from date scan completed)	July 30, 2023
Compliance status:	PASS	Scan report type	Full Scan
Number of unique in-scope components[4] scanned			67
Number of identified failing vulnerabilities			0
Number of components found by ASV but not scanned because scan customer confirmed components were out of scope			0

[4] A Components includes any host, virtual host, IP address, FQDN or unique vector into a system or cardholder data environment.

Exhibit 10R

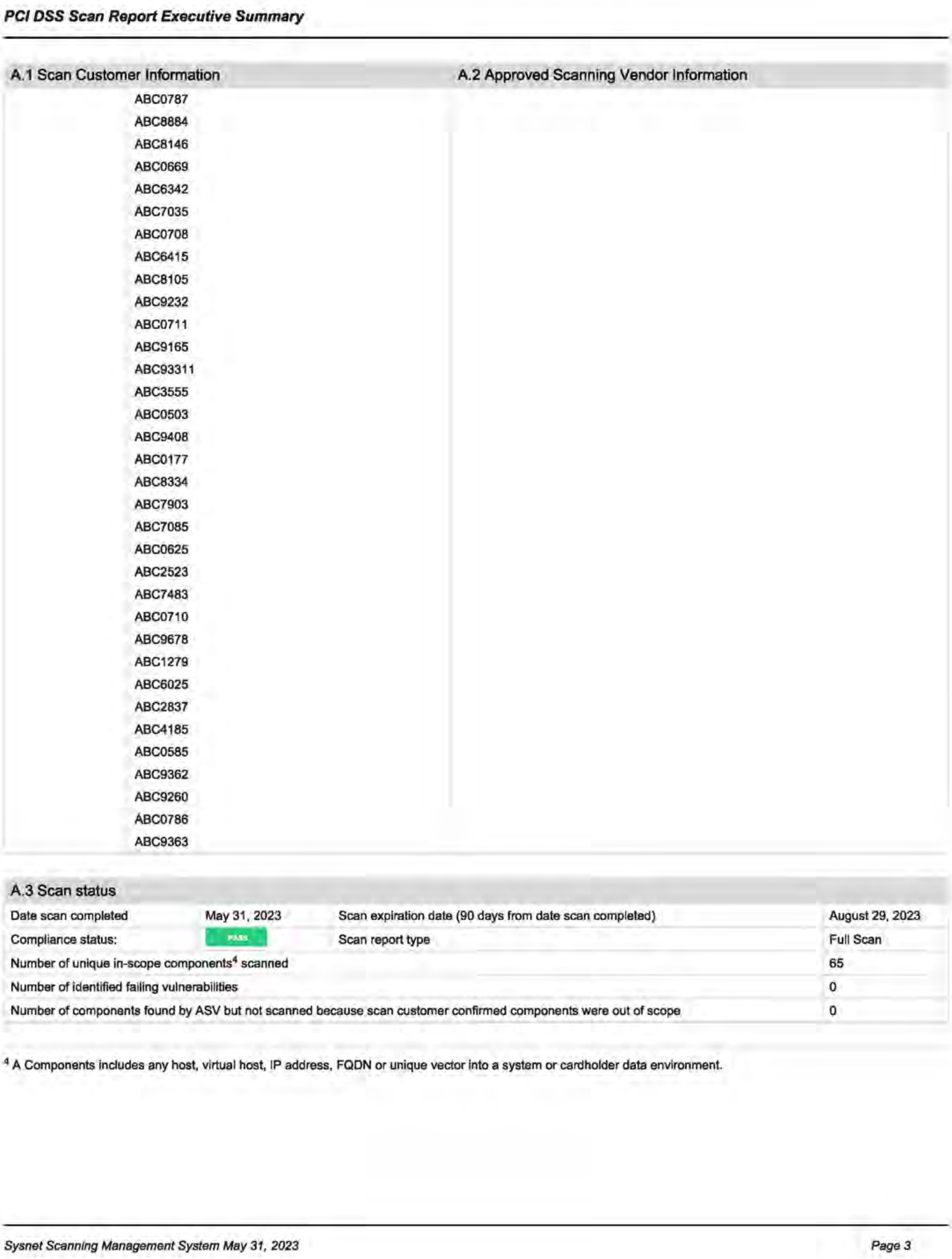
PCI DSS Scan Report Executive Summary

Exhibit 10R

sysnet. global solutions Powered by Qualys.

A.1 Scan Customer Information				A.2 Approved Scanning Vendor Information			
Company:	G0007 PLANET FITNESS BRICK			Company:	Sysnet		
Contact:	Ryan Wagner	Title:		Contact:	gopi balachenna	Title:	ASV
Telephone:		Email:	ryan.wagner@pfgrwth.com	Telephone:	+35314951300	Email:	balachenna.gopi@sysnetgs.com
Business address:	5425 BALTIMORE NTL PIKE BALTIMORE Maryland			Business address:	4th Floor The Herbert Building Carrickmines Dublin 18 Republic Of Ireland		
URL:				URL:	www.sysnetglobalsolutions.com		
MID:	ABC0325						
Other Mids covered by this scan result	ABC0707 ABC0838 ABC2738 ABC0906 ABC0914 ABC6063 ABC0907 ABC9539 ABC6905 ABC0929 ABC9351 ABC8702 ABC0963 ABC8076 ABC0877 ABC9120 ABC0695 ABC0469 ABC9318 ABC9358 ABC8091 ABC8127 ABC0349 ABC1763 ABC0263 ABC6523 ABC7211 ABC0706 ABC0709 ABC7086 ABC0705 ABC93088 ABC0888 ABC5263 ABC9308 ABC7606 ABC8585 ABC7246						

Exhibit 10R



A.1 Scan Customer Information	A.2 Approved Scanning Vendor Information
ABC0787	
ABC8884	
ABC8146	
ABC0669	
ABC6342	
ABC7035	
ABC0708	
ABC6415	
ABC8105	
ABC9232	
ABC0711	
ABC9165	
ABC93311	
ABC3555	
ABC0503	
ABC9408	
ABC0177	
ABC8334	
ABC7903	
ABC7085	
ABC0625	
ABC2523	
ABC7483	
ABC0710	
ABC9678	
ABC1279	
ABC6025	
ABC2837	
ABC4185	
ABC0585	
ABC9362	
ABC9260	
ABC0786	
ABC9363	

A.3 Scan status

Date scan completed	May 31, 2023	Scan expiration date (90 days from date scan completed)	August 29, 2023
Compliance status:	PASS	Scan report type	Full Scan
Number of unique in-scope components[4] scanned			65
Number of identified failing vulnerabilities			0
Number of components found by ASV but not scanned because scan customer confirmed components were out of scope			0

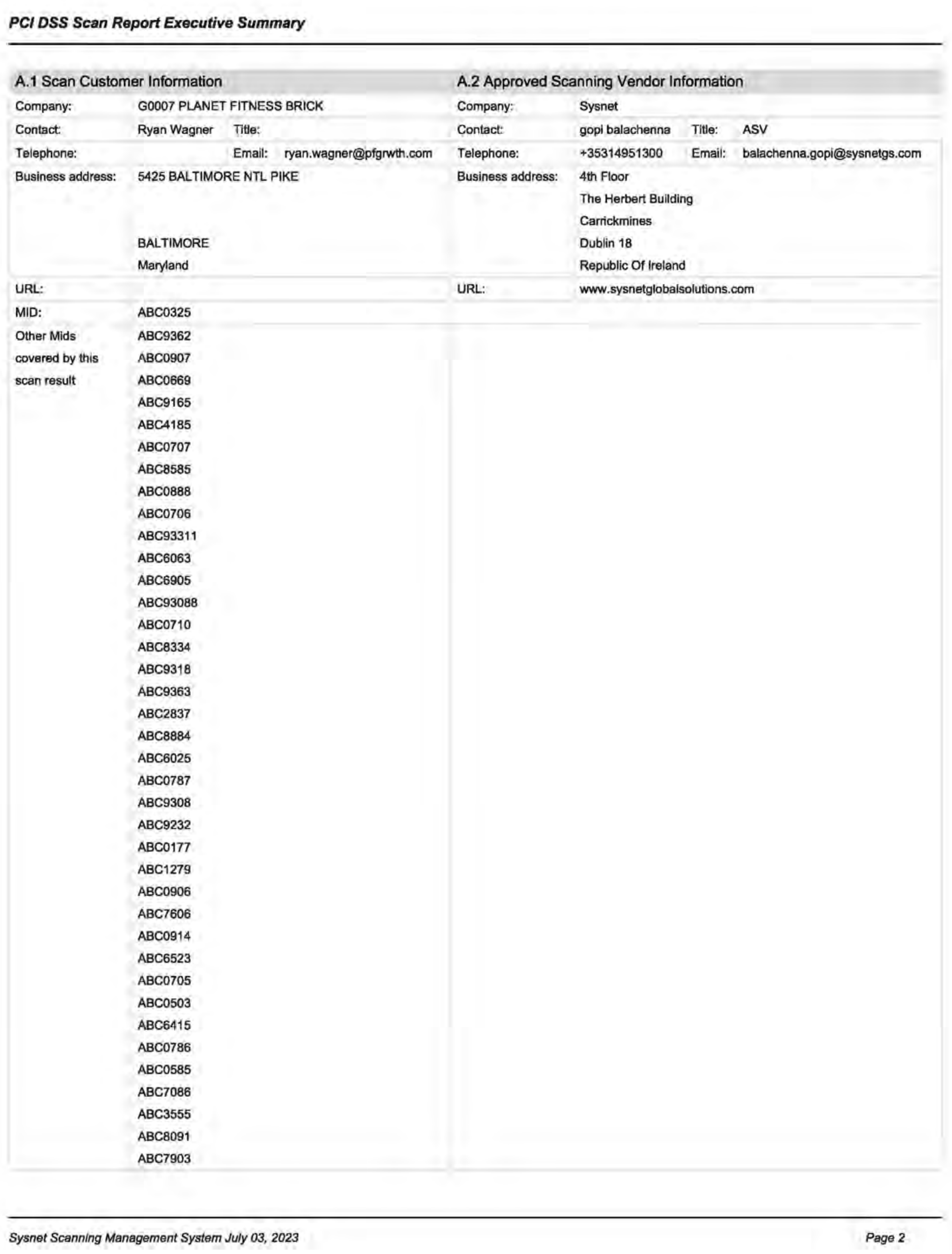
[4] A Components includes any host, virtual host, IP address, FQDN or unique vector into a system or cardholder data environment.

Exhibit 10R

PCI DSS Scan Report Executive Summary

sysnet. global solutions Powered by Qualys.

Exhibit 10R



A.1 Scan Customer Information

Company:	G0007 PLANET FITNESS BRICK		
Contact:	Ryan Wagner	Title:	
Telephone:		Email:	ryan.wagner@pfgrwth.com
Business address:	5425 BALTIMORE NTL PIKE BALTIMORE Maryland		
URL:			
MID:	ABC0325		
Other Mids covered by this scan result	ABC9362 ABC0907 ABC0669 ABC9165 ABC4185 ABC0707 ABC8585 ABC0888 ABC0706 ABC93311 ABC6063 ABC6905 ABC93088 ABC0710 ABC8334 ABC9318 ABC9363 ABC2837 ABC8884 ABC6025 ABC0787 ABC9308 ABC9232 ABC0177 ABC1279 ABC0906 ABC7606 ABC0914 ABC6523 ABC0705 ABC0503 ABC6415 ABC0786 ABC0585 ABC7086 ABC3555 ABC8091 ABC7903		

A.2 Approved Scanning Vendor Information

Company:	Sysnet		
Contact:	gopi balachenna	Title:	ASV
Telephone:	+35314951300	Email:	balachenna.gopi@sysnetgs.com
Business address:	4th Floor The Herbert Building Carrickmines Dublin 18 Republic Of Ireland		
URL:	www.sysnetglobalsolutions.com		

Exhibit 10R

A.1 Scan Customer Information	A.2 Approved Scanning Vendor Information
ABC1763	
ABC0929	
ABC8127	
ABC7246	
ABC9120	
ABC0625	
ABC9358	
ABC7085	
ABC7211	
ABC8702	
ABC0709	
ABC0469	
ABC9678	
ABC0877	
ABC8105	
ABC8146	
ABC0695	
ABC0263	
ABC8076	
ABC0711	
ABC9260	
ABC9539	
ABC0708	
ABC0349	
ABC9408	
ABC0963	
ABC5263	
ABC6342	
ABC9351	
ABC2523	
ABC7483	
ABC0838	
ABC7035	
ABC2738	

Exhibit 10R

A.3 Scan status

Date scan completed	June 30, 2023	Scan expiration date (90 days from date scan completed)	September 28, 2023
Compliance status:	PASS	Scan report type	Full Scan
Number of unique in-scope components[4] scanned			63
Number of identified failing vulnerabilities			0
Number of components found by ASV but not scanned because scan customer confirmed components were out of scope			0

[4] A Components includes any host, virtual host, IP address, FQDN or unique vector into a system or cardholder data environment.

PCI DSS Scan Report Executive Summary

Exhibit 10R

sysnet global solutions Powered by Qualys.

A.1 Scan Customer Information			
Company:	G0007 PLANET FITNESS BRICK		
Contact:	Ryan Wagner	Title:	
Telephone:	410-252-8058 x109	Email:	ITO@ohanagp.com
Business address:	5425 BALTIMORE NTL PIKE BALTIMORE Maryland		
URL:			
MID:	ABC0325		
Other Mids covered by this scan result	ABC0786 ABC8091 ABC2837 ABC0177 ABC0263 ABC9120 ABC0914 ABC6025 ABC9678 ABC0877 ABC8105 ABC7211 ABC0710 ABC0708 ABC93311 ABC0906 ABC9362 ABC7903 ABC2523 ABC0706 ABC8334 ABC93088 ABC9165 ABC8884 ABC0503 ABC0707 ABC9351 ABC8127 ABC7086 ABC9539 ABC4185 ABC9408 ABC6063 ABC0349 ABC0469 ABC9358 ABC0963 ABC6342		

A.2 Approved Scanning Vendor Information			
Company:	Sysnet		
Contact:	gopi balachenna	Title:	ASV
Telephone:	+35314951300	Email:	balachenna.gopi@sysnetgs.com
Business address:	4th Floor The Herbert Building Carrickmines Dublin 18 Republic Of Ireland		
URL:	www.sysnetglobalsolutions.com		

Exhibit 10R

A.1 Scan Customer Information	A.2 Approved Scanning Vendor Information
ABC0695	
ABC9318	
ABC1279	
ABC0705	
ABC0625	
ABC1763	
ABC3555	
ABC5263	
ABC6905	
ABC0787	
ABC0669	
ABC0929	
ABC9232	
ABC9308	
ABC0709	
ABC9260	
ABC0585	
ABC7246	
ABC0711	
ABC8702	
ABC8585	
ABC7085	
ABC0907	
ABC7035	
ABC2738	
ABC6415	
ABC8076	
ABC7606	
ABC6523	
ABC0838	
ABC7483	
ABC9363	
ABC0888	
ABC8146	

A.3 Scan status

Date scan completed	July 31, 2023	Scan expiration date (90 days from date scan completed)	October 29, 2023
Compliance status:	PASS	Scan report type	Full Scan
Number of unique in-scope components[4] scanned			62
Number of identified failing vulnerabilities			0
Number of components found by ASV but not scanned because scan customer confirmed components were out of scope			0

[4] A Components includes any host, virtual host, IP address, FQDN or unique vector into a system or cardholder data environment.

Exhibit 10R

PCI DSS Scan Report Executive Summary

Exhibit 10R

sysnet global solutions Powered by Qualys.

A.1 Scan Customer Information

Company:	G0007 PLANET FITNESS BRICK		
Contact:	Ryan Wagner	Title:	
Telephone:	410-252-8058 x109	Email:	ITO@ohanagp.com
Business address:	5425 BALTIMORE NTL PIKE BALTIMORE Maryland		
URL:			
MID:	ABC0325		
Other Mids covered by this scan result	ABC8091 ABC7086 ABC0177 ABC6905 ABC9165 ABC0711 ABC2523 ABC9308 ABC0709 ABC3555 ABC9358 ABC93311 ABC0469 ABC8334 ABC9120 ABC0705 ABC8702 ABC6342 ABC0625 ABC6523 ABC9363 ABC6025 ABC2738 ABC7035 ABC0710 ABC5263 ABC0906 ABC9232 ABC0929 ABC8127 ABC0914 ABC8076 ABC0838 ABC0349 ABC9678 ABC0695 ABC8585 ABC93088		

A.2 Approved Scanning Vendor Information

Company:	Sysnet		
Contact:	gopi balachenna	Title:	ASV
Telephone:	+35314951300	Email:	balachenna.gopi@sysnetgs.com
Business address:	4th Floor The Herbert Building Carrickmines Dublin 18 Republic Of Ireland		
URL:	www.sysnetglobalsolutions.com		

Exhibit 10R

A.1 Scan Customer Information	A.2 Approved Scanning Vendor Information
ABC0907	
ABC2837	
ABC6415	
ABC8146	
ABC7246	
ABC8105	
ABC0888	
ABC0585	
ABC7483	
ABC0707	
ABC1279	
ABC9408	
ABC9260	
ABC9362	
ABC7085	
ABC7903	
ABC6063	
ABC0708	
ABC7211	
ABC0706	
ABC0669	
ABC9351	
ABC9539	
ABC9318	
ABC0263	
ABC4185	
ABC7606	
ABC0877	
ABC0786	
ABC0503	
ABC0963	
ABC0787	
ABC1763	
ABC8884	

Exhibit 10R

A.3 Scan status

Date scan completed	September 01, 2023	Scan expiration date (90 days from date scan completed)	November 30, 2023
Compliance status:	PASS	Scan report type	Full Scan
Number of unique in-scope components[4] scanned			60
Number of identified failing vulnerabilities			0
Number of components found by ASV but not scanned because scan customer confirmed components were out of scope			0

[4] A Components includes any host, virtual host, IP address, FQDN or unique vector into a system or cardholder data environment.

PCI DSS Scan Report Executive Summary

sysnet global solutions Powered by Qualys.

Exhibit 10R

PCI DSS Scan Report Executive Summary

Exhibit 10R

A.1 Scan Customer Information

Company:	G0007 PLANET FITNESS BRICK		
Contact:	Ryan Wagner	Title:	
Telephone:	410-252-8058 x109	Email:	ITO@ohanagp.com
Business address:	5425 BALTIMORE NTL PIKE BALTIMORE Maryland		
URL:			
MID:	ABC0325		
Other Mids covered by this scan result	ABC0877 ABC9358 ABC0469 ABC9362 ABC7606 ABC7085 ABC8076 ABC1279 ABC0349 ABC0695 ABC0906 ABC0707 ABC0625 ABC8146 ABC9232 ABC6025 ABC0711 ABC0907 ABC93311 ABC0706 ABC6063 ABC6415 ABC2523 ABC0585 ABC8334 ABC0914 ABC2738 ABC0963 ABC8127 ABC0669 ABC0786 ABC9539 ABC8702 ABC3555 ABC0888 ABC5263 ABC8884 ABC4185		

A.2 Approved Scanning Vendor Information

Company:	Sysnet		
Contact:	gopi balachenna	Title:	ASV
Telephone:	+35314951300	Email:	balachenna.gopi@sysnetgs.com
Business address:	4th Floor The Herbert Building Carrickmines Dublin 18 Republic Of Ireland		
URL:	www.sysnetglobalsolutions.com		

A.1 Scan Customer Information

ABC1763
ABC6523
ABC7086
ABC93088
ABC0929
ABC8585
ABC0709
ABC6342
ABC9165
ABC9678
ABC0503
ABC9363
ABC7903
ABC0177
ABC0263
ABC8105
ABC7211
ABC9351
ABC0710
ABC2837
ABC0708
ABC9308
ABC7246
ABC9120
ABC7035
ABC9408
ABC0838
ABC8091
ABC9260
ABC0787
ABC0705
ABC7483
ABC9318
ABC6905

A.2 Approved Scanning Vendor Information

A.3 Scan status

Date scan completed	October 01, 2023	Scan expiration date (90 days from date scan completed)	December 30, 2023
Compliance status:	PASS	Scan report type	Full Scan
Number of unique in-scope components[4] scanned			60
Number of identified failing vulnerabilities			0
Number of components found by ASV but not scanned because scan customer confirmed components were out of scope			0

[4] A Components includes any host, virtual host, IP address, FQDN or unique vector into a system or cardholder data environment.

Exhibit 10R

PCI DSS Scan Report Executive Summary

Exhibit 10R

sysnet global solutions Powered by Qualys.

A.1 Scan Customer Information				A.2 Approved Scanning Vendor Information			
Company:	G0007 PLANET FITNESS BRICK			Company:	Sysnet		
Contact:	Ryan Wagner	Title:		Contact:	gopi balachenna	Title:	ASV
Telephone:	410-252-8058 x109	Email:	ITO@ohanagp.com	Telephone:	+35314951300	Email:	balachenna.gopi@sysnetgs.com
Business address:	5425 BALTIMORE NTL PIKE BALTIMORE Maryland			Business address:	4th Floor The Herbert Building Carrickmines Dublin 18 Republic Of Ireland		
URL:				URL:	www.sysnetglobalsolutions.com		
MID:	ABC0325						
Other Mids covered by this scan result	ABC9363 ABC8146 ABC9539 ABC0708 ABC9351 ABC0710 ABC2523 ABC9232 ABC1763 ABC0786 ABC0669 ABC9260 ABC0709 ABC7086 ABC9308 ABC0707 ABC0585 ABC7903 ABC7035 ABC6342 ABC6523 ABC8884 ABC6063 ABC9165 ABC0695 ABC8091 ABC8076 ABC2738 ABC1279 ABC0888 ABC8105 ABC0177 ABC0787 ABC9678 ABC0469 ABC0914 ABC0625 ABC2837						

Exhibit 10R

A.1 Scan Customer Information	A.2 Approved Scanning Vendor Information
ABC9318	
ABC8585	
ABC9408	
ABC0906	
ABC93088	
ABC0838	
ABC4185	
ABC93311	
ABC3555	
ABC0907	
ABC7211	
ABC0349	
ABC0263	
ABC0929	
ABC8127	
ABC0503	
ABC0706	
ABC9358	
ABC7606	
ABC9362	
ABC6415	
ABC6025	
ABC5263	
ABC8702	
ABC8334	
ABC0877	
ABC7246	
ABC6905	
ABC0711	
ABC0963	
ABC0705	
ABC9120	
ABC7085	
ABC7483	

Exhibit 10R

A.3 Scan status

Date scan completed	December 04, 2023	Scan expiration date (90 days from date scan completed)	March 03, 2024
Compliance status:	PASS	Scan report type	Full Scan
Number of unique in-scope components[4] scanned			74
Number of identified failing vulnerabilities			0
Number of components found by ASV but not scanned because scan customer confirmed components were out of scope			0

[4] A Components includes any host, virtual host, IP address, FQDN or unique vector into a system or cardholder data environment.

PCI DSS Scan Report Executive Summary

Exhibit 10R

sysnet global solutions Powered by Qualys.

A.1 Scan Customer Information

Company:	G0007 PLANET FITNESS BRICK		
Contact:	Ryan Wagner	Title:	
Telephone:	410-252-8058 x109	Email:	ITO@ohanagp.com
Business address:	5425 BALTIMORE NTL PIKE BALTIMORE Maryland		
URL:			
MID:	ABC0325		
Other Mids covered by this scan result	ABC0705 ABC93311 ABC6523 ABC8884 ABC7085 ABC7483 ABC7246 ABC0907 ABC9165 ABC0914 ABC0906 ABC9351 ABC8702 ABC9260 ABC0695 ABC0177 ABC2837 ABC8146 ABC7903 ABC9232 ABC7211 ABC0263 ABC0708 ABC0838 ABC2738 ABC8076 ABC6342 ABC0710 ABC0503 ABC3555 ABC0625 ABC0888 ABC6905 ABC0707 ABC6025 ABC0585 ABC0786 ABC6415		

A.2 Approved Scanning Vendor Information

Company:	Sysnet		
Contact:	gopi balachenna	Title:	ASV
Telephone:	+35314951300	Email:	balachenna.gopi@sysnetgs.com
Business address:	4th Floor The Herbert Building Carrickmines Dublin 18 Republic Of Ireland		
URL:	www.sysnetglobalsolutions.com		

Exhibit 10R

A.1 Scan Customer Information	A.2 Approved Scanning Vendor Information
ABC6063	
ABC0349	
ABC9678	
ABC8105	
ABC8091	
ABC5263	
ABC7035	
ABC4185	
ABC0787	
ABC9408	
ABC8127	
ABC0669	
ABC0929	
ABC8585	
ABC9358	
ABC7086	
ABC93088	
ABC8334	
ABC9362	
ABC9363	
ABC1279	
ABC9318	
ABC1763	
ABC0469	
ABC2523	
ABC0877	
ABC0706	
ABC7606	
ABC9539	
ABC0963	
ABC0709	
ABC9120	
ABC9308	
ABC0711	

A.3 Scan status

Date scan completed	January 01, 2024	Scan expiration date (90 days from date scan completed)	March 31, 2024
Compliance status:	PASS	Scan report type	Full Scan
Number of unique in-scope components[4] scanned			76
Number of identified failing vulnerabilities			0
Number of components found by ASV but not scanned because scan customer confirmed components were out of scope			0

[4] A Components includes any host, virtual host, IP address, FQDN or unique vector into a system or cardholder data environment.

Exhibit 10R

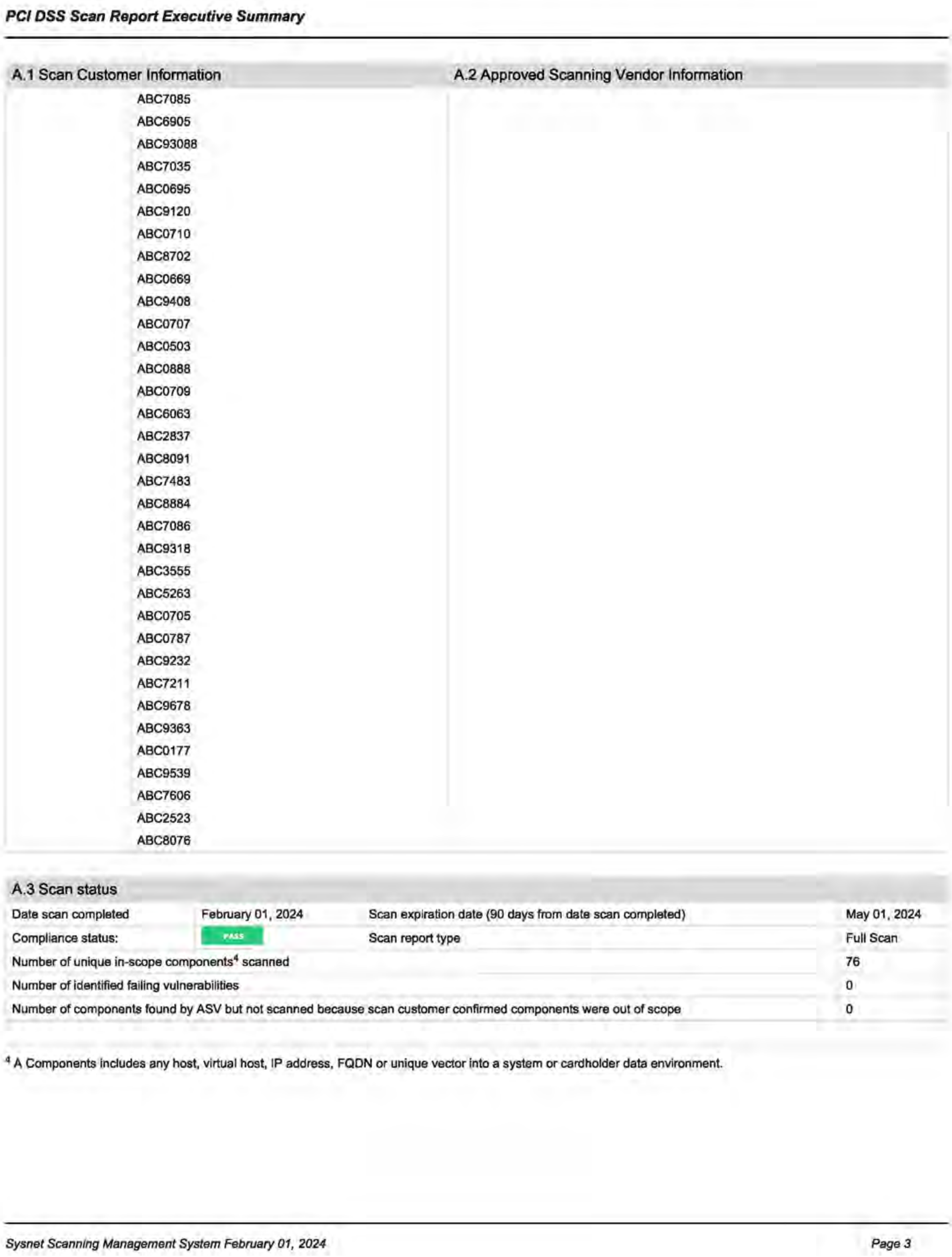
PCI DSS Scan Report Executive Summary

Exhibit 10R

sysnet global solutions Powered by Qualys.

A.1 Scan Customer Information				A.2 Approved Scanning Vendor Information			
Company:	G0007 PLANET FITNESS BRICK			Company:	Sysnet		
Contact:	Ryan Wagner	Title:		Contact:	gopi balachenna	Title:	ASV
Telephone:	410-252-8058 x109	Email:	ITO@ohanagp.com	Telephone:	+35314951300	Email:	balachenna.gopi@sysnetgs.com
Business address:	5425 BALTIMORE NTL PIKE BALTIMORE Maryland			Business address:	4th Floor The Herbert Building Carrickmines Dublin 18 Republic Of Ireland		
URL:				URL:	www.sysnetglobalsolutions.com		
MID:	ABC0325						
Other Mids covered by this scan result	ABC2738 ABC6415 ABC0914 ABC9362 ABC0625 ABC0786 ABC8105 ABC0469 ABC0877 ABC9165 ABC6523 ABC0711 ABC9260 ABC4185 ABC8334 ABC0838 ABC7246 ABC9351 ABC0929 ABC0349 ABC8127 ABC0708 ABC6025 ABC0263 ABC0963 ABC8146 ABC9358 ABC8585 ABC7903 ABC0906 ABC6342 ABC93311 ABC0706 ABC1763 ABC0907 ABC9308 ABC1279 ABC0585						

Exhibit 10R



A.1 Scan Customer Information

ABC7085
ABC6905
ABC93088
ABC7035
ABC0695
ABC9120
ABC0710
ABC8702
ABC0669
ABC9408
ABC0707
ABC0503
ABC0888
ABC0709
ABC6063
ABC2837
ABC8091
ABC7483
ABC8884
ABC7086
ABC9318
ABC3555
ABC5263
ABC0705
ABC0787
ABC9232
ABC7211
ABC9678
ABC9363
ABC0177
ABC9539
ABC7606
ABC2523
ABC8076

A.2 Approved Scanning Vendor Information

A.3 Scan status

Date scan completed	February 01, 2024	Scan expiration date (90 days from date scan completed)	May 01, 2024
Compliance status:	PASS	Scan report type	Full Scan
Number of unique in-scope components[4] scanned			76
Number of identified failing vulnerabilities			0
Number of components found by ASV but not scanned because scan customer confirmed components were out of scope			0

[4] A Components includes any host, virtual host, IP address, FQDN or unique vector into a system or cardholder data environment.

Exhibit 10R

PCI DSS Scan Report Executive Summary

Exhibit 10R

sysnet global solutions Powered by Qualys.

A.1 Scan Customer Information				**A.2 Approved Scanning Vendor Information**			
Company:	G0007 PLANET FITNESS BRICK			Company:	Sysnet		
Contact:	Ryan Wagner	Title:		Contact:	gopi balachenna	Title:	ASV
Telephone:	410-252-8058 x109	Email:	ITO@ohanagp.com	Telephone:	+35314951300	Email:	balachenna.gopi@sysnetgs.com
Business address:	5425 BALTIMORE NTL PIKE BALTIMORE Maryland			Business address:	4th Floor The Herbert Building Carrickmines Dublin 18 Republic Of Ireland		
URL:				URL:	www.sysnetglobalsolutions.com		
MID:	ABC0325						
Other Mids covered by this scan result	ABC8076 ABC9120 ABC6342 ABC0711 ABC0838 ABC6025 ABC8127 ABC0888 ABC0503 ABC4185 ABC9165 ABC0709 ABC7085 ABC9363 ABC9408 ABC0906 ABC8105 ABC3555 ABC93088 ABC0914 ABC0787 ABC0585 ABC7606 ABC1279 ABC0710 ABC8146 ABC7035 ABC0263 ABC2738 ABC8585 ABC9351 ABC7483 ABC7086 ABC8702 ABC7903 ABC9318 ABC5263 ABC93311						

Exhibit 10R

A.1 Scan Customer Information

ABC6523
ABC9539
ABC7211
ABC0707
ABC2523
ABC2837
ABC0177
ABC0695
ABC9260
ABC9362
ABC6415
ABC0669
ABC0907
ABC0929
ABC0705
ABC9358
ABC8884
ABC9678
ABC0786
ABC0469
ABC6905
ABC9232
ABC1763
ABC0349
ABC0708
ABC8091
ABC9308
ABC0625
ABC6063
ABC7246
ABC0706
ABC0877
ABC0963
ABC8334

A.2 Approved Scanning Vendor Information

A.3 Scan status

Date scan completed	March 02, 2024	Scan expiration date (90 days from date scan completed)	May 31, 2024
Compliance status:	PASS	Scan report type	Full Scan
Number of unique in-scope components[4] scanned			75
Number of identified failing vulnerabilities			0
Number of components found by ASV but not scanned because scan customer confirmed components were out of scope			0

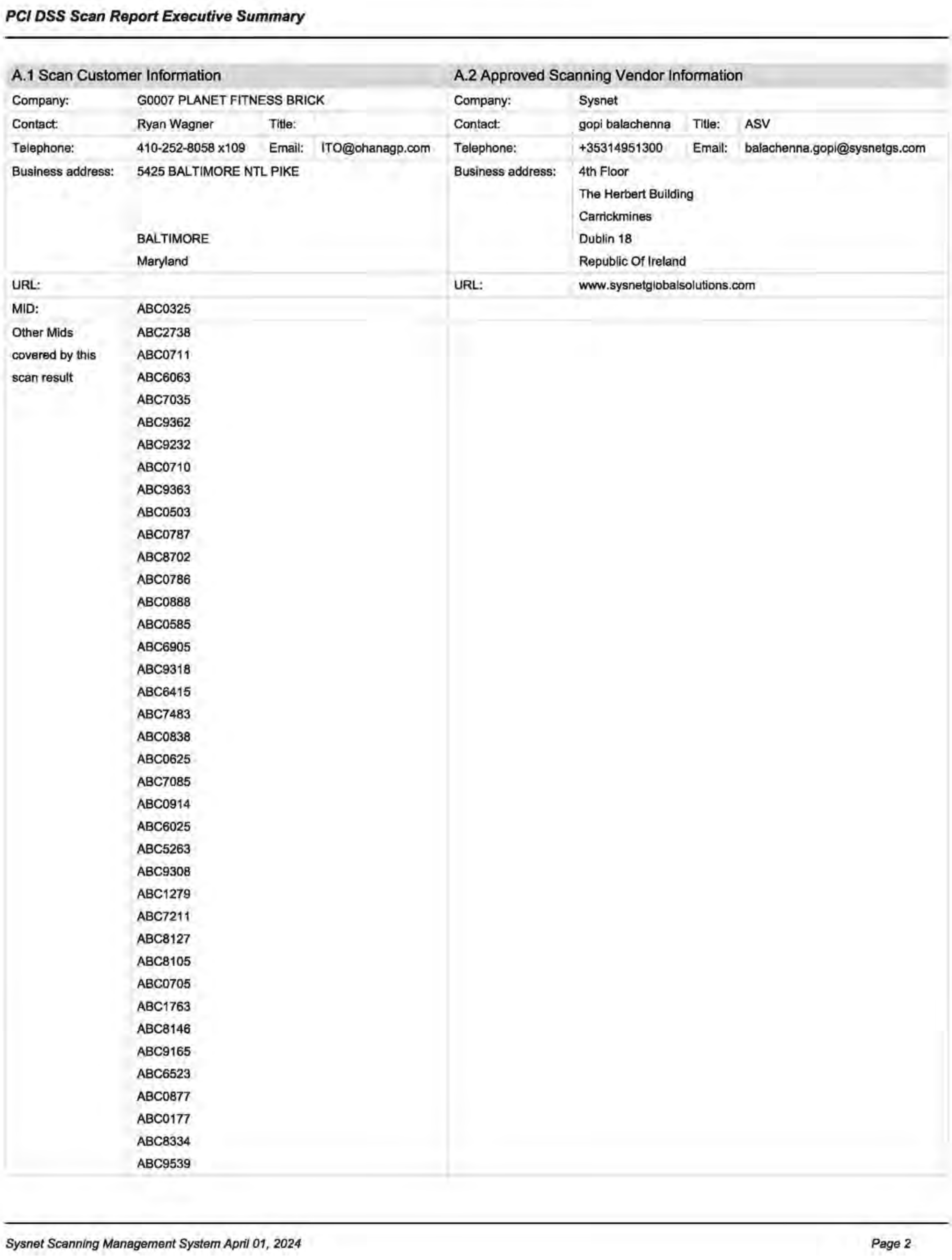
[4] A Components includes any host, virtual host, IP address, FQDN or unique vector into a system or cardholder data environment.

Exhibit 10R

PCI DSS Scan Report Executive Summary

Exhibit 10R

sysnet. global solutions Powered by Qualys.



A.1 Scan Customer Information				A.2 Approved Scanning Vendor Information			
Company:	G0007 PLANET FITNESS BRICK			Company:	Sysnet		
Contact:	Ryan Wagner	Title:		Contact:	gopi balachenna	Title:	ASV
Telephone:	410-252-8058 x109	Email:	ITO@ohanagp.com	Telephone:	+35314951300	Email:	balachenna.gopi@sysnetgs.com
Business address:	5425 BALTIMORE NTL PIKE BALTIMORE Maryland			Business address:	4th Floor The Herbert Building Carrickmines Dublin 18 Republic Of Ireland		
URL:				URL:	www.sysnetglobalsolutions.com		
MID:	ABC0325						
Other Mids covered by this scan result	ABC2738 ABC0711 ABC6063 ABC7035 ABC9362 ABC9232 ABC0710 ABC9363 ABC0503 ABC0787 ABC8702 ABC0786 ABC0888 ABC0585 ABC6905 ABC9318 ABC6415 ABC7483 ABC0838 ABC0625 ABC7085 ABC0914 ABC6025 ABC5263 ABC9308 ABC1279 ABC7211 ABC8127 ABC8105 ABC0705 ABC1763 ABC8146 ABC9165 ABC6523 ABC0877 ABC0177 ABC8334 ABC9539						

Exhibit 10R

A.1 Scan Customer Information	A.2 Approved Scanning Vendor Information
ABC4185	
ABC2837	
ABC3555	
ABC7086	
ABC0907	
ABC9358	
ABC0906	
ABC0708	
ABC2523	
ABC0929	
ABC0263	
ABC0669	
ABC7246	
ABC0709	
ABC9408	
ABC0707	
ABC0349	
ABC9678	
ABC8076	
ABC8585	
ABC0469	
ABC9260	
ABC9351	
ABC0706	
ABC93088	
ABC93311	
ABC8884	
ABC9120	
ABC8091	
ABC0695	
ABC7606	
ABC0963	
ABC6342	
ABC7903	

A.3 Scan status

Date scan completed	April 01, 2024	Scan expiration date (90 days from date scan completed)	June 30, 2024
Compliance status:	🟩 PASS	Scan report type	Full Scan
Number of unique in-scope components[4] scanned			77
Number of identified failing vulnerabilities			0
Number of components found by ASV but not scanned because scan customer confirmed components were out of scope			0

[4] A Components includes any host, virtual host, IP address, FQDN or unique vector into a system or cardholder data environment.

Exhibit 10R

PCI DSS Scan Report Executive Summary

Exhibit 10R

sysnet global solutions Powered by Qualys.

A.1 Scan Customer Information

Company:	G0007 PLANET FITNESS BRICK		
Contact:	Ryan Wagner	Title:	
Telephone:	410-252-8058 x109	Email:	ITO@ohanagp.com
Business address:	5425 BALTIMORE NTL PIKE BALTIMORE Maryland		
URL:			
MID:	ABC0325		
Other Mids covered by this scan result	ABC7606 ABC0877 ABC7246 ABC0888 ABC6905 ABC7086 ABC0914 ABC0707 ABC0710 ABC0503 ABC4185 ABC8127 ABC9318 ABC8585 ABC9120 ABC8702 ABC93088 ABC0695 ABC0263 ABC3555 ABC8091 ABC6342 ABC9351 ABC0585 ABC0907 ABC0709 ABC9363 ABC0711 ABC9678 ABC8076 ABC0838 ABC0705 ABC0625 ABC7483 ABC9362 ABC8146 ABC0177 ABC8105		

A.2 Approved Scanning Vendor Information

Company:	Sysnet		
Contact:	gopi balachenna	Title:	ASV
Telephone:	+35314951300	Email:	balachenna.gopi@sysnetgs.com
Business address:	4th Floor The Herbert Building Carrickmines Dublin 18 Republic Of Ireland		
URL:	www.sysnetglobalsolutions.com		

Exhibit 10R

A.1 Scan Customer Information

ABC9408
ABC7085
ABC5263
ABC0349
ABC93311
ABC1279
ABC9539
ABC8884
ABC6523
ABC7903
ABC9308
ABC2837
ABC6415
ABC2523
ABC8334
ABC0906
ABC0929
ABC0469
ABC7211
ABC9358
ABC9165
ABC1763
ABC6025
ABC0787
ABC0786
ABC0708
ABC2738
ABC0669
ABC9260
ABC0706
ABC7035
ABC0963
ABC9232
ABC6063

A.2 Approved Scanning Vendor Information

A.3 Scan status

Date scan completed	May 01, 2024	Scan expiration date (90 days from date scan completed)	July 30, 2024
Compliance status:	PASS	Scan report type	Full Scan
Number of unique in-scope components[4] scanned			78
Number of identified failing vulnerabilities			0
Number of components found by ASV but not scanned because scan customer confirmed components were out of scope			0

[4] A Components includes any host, virtual host, IP address, FQDN or unique vector into a system or cardholder data environment.

Exhibit 10R

Exhibit 22A-1

Build and Maintain a Secure Network and Systems

Requirement 1: Install and Maintain Network Security Controls

Sections	
1.1	Processes and mechanisms for installing and maintaining network security controls are defined and understood.
1.2	Network security controls (NSCs) are configured and maintained.
1.3	Network access to and from the cardholder data environment is restricted.
1.4	Network connections between trusted and untrusted networks are controlled.
1.5	Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.

Exhibit 22A-1

Overview

Network security controls (NSCs), such as firewalls and other network security technologies, are network policy enforcement points that typically control network traffic between two or more logical or physical network segments (or subnets) based on pre-defined *policies* or *rules*.

NSCs examine all network traffic entering (ingress) and leaving (egress) a segment and decide, based on the policies defined, whether the network traffic is allowed to pass or whether it should be rejected. Typically, NSCs are placed between environments with different security needs or levels of trust, however in some environments NSCs control the traffic to individual devices irrespective of trust boundaries. Policy enforcement generally occurs at layer 3 of the OSI model, but data present in higher layers is also frequently used to determine policy decisions.

Traditionally this function has been provided by physical firewalls; however, now this functionality may be provided by virtual devices, cloud access controls, virtualization/container systems, and other software-defined networking technology.

NSCs are used to control traffic within an entity's own networks—for example, between highly sensitive and less sensitive areas—and also to protect the entity's resources from exposure to untrusted networks. The cardholder data environment (CDE) is an example of a more sensitive area within an entity's network. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into sensitive systems. NSCs provide a key protection mechanism for any computer network.

Common examples of untrusted networks include the Internet, dedicated connections such as business-to-business communication channels, wireless networks, carrier networks (such as cellular), third-party networks, and other sources outside the entity's ability to control. Furthermore, untrusted networks also include corporate networks that are considered out-of-scope for PCI DSS, because they are not assessed, and therefore must be treated as untrusted because the existence of security controls has not been verified. While an entity may consider an internal network to be trusted from an infrastructure perspective, if a network is out of scope for PCI DSS, that network must be considered untrusted for PCI DSS.

Refer to *Appendix G* for definitions of PCI DSS terms.

Exhibit 22A-1

Requirements and Testing Procedures		Guidance
1.1 Processes and mechanisms for installing and maintaining network security controls are defined and understood.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Requirement 1.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 1. While it is important to define the specific policies or procedures called out in Requirement 1, it is equally important to ensure they are properly documented, maintained, and disseminated. **Good Practice** It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For these reasons, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle. **Definitions** Security policies define the entity's security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives.
1.1.1 All security policies and operational procedures that are identified in Requirement 1 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	**1.**1.1 Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 1 are managed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Expectations, controls, and oversight for meeting activities within Requirement 1 are defined, understood, and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.		

Exhibit 22A-1

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and critical activities may not occur. **Good Practice** Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities. **Examples** A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).
1.1.2 Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood.	**1.1.2.a** Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 1 are documented and assigned.	
	1.1.2.b Interview personnel responsible for performing activities in Requirement 1 to verify that roles and responsibilities are assigned as documented and are understood.	
Customized Approach Objective		
Day-to-day responsibilities for performing all the activities in Requirement 1 are allocated. Personnel are accountable for successful, continuous operation of these requirements.		

Exhibit 22A-1

Requirements and Testing Procedures		Guidance
1.2 Network security controls (NSCs) are configured and maintained.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** The implementation of these configuration standards results in the NSC being configured and managed to properly perform their security function (often referred to as the ruleset). **Good Practice** These standards often define the requirements for acceptable protocols, ports that are permitted to be used, and specific configuration requirements that are acceptable. Configuration standards may also outline what the entity considers not acceptable or not permitted within its network. **Definitions** NSCs are key components of a network architecture. Most commonly, NSCs are used at the boundaries of the CDE to control network traffic flowing inbound and outbound from the CDE. Configuration standards outline an entity's minimum requirements for the configuration of its NSCs. **Examples** Examples of NSCs covered by these configuration standards include, but are not limited to, firewalls, routers configured with access control lists, and cloud virtual networks.
1.2.1 Configuration standards for NSC rulesets are: • Defined. • Implemented. • Maintained.	**1.2.1.a** Examine the configuration standards for NSC rulesets to verify the standards are in accordance with all elements specified in this requirement.	
	1.2.1.b Examine configuration settings for NSC rulesets to verify that rulesets are implemented according to the configuration standards.	
Customized Approach Objective		
The way that NSCs are configured and operate are defined and consistently applied.		

Exhibit 22A-1

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Following a structured change control process for all changes to NSCs reduces the risk that a change could introduce a security vulnerability. **Good Practice** Changes should be approved by individuals with the appropriate authority and knowledge to understand the impact of the change. Verification should provide reasonable assurance that the change did not adversely impact the security of the network and that the change performs as expected. To avoid having to address security issues introduced by a change, all changes should be approved prior to being implemented and verified after the change is implemented. Once approved and verified, network documentation should be updated to include the changes to prevent inconsistencies between network documentation and the actual configuration.
1.2.2 All changes to network connections and to configurations of NSCs are approved and managed in accordance with the change control process defined at Requirement 6.5.1.	**1.2.2.a** Examine documented procedures to verify that changes to network connections and configurations of NSCs are included in the formal change control process in accordance with Requirement 6.5.1.	
	1.2.2.b Examine network configuration settings to identify changes made to network connections. Interview responsible personnel and examine change control records to verify that identified changes to network connections were approved and managed in accordance with Requirement 6.5.1.	
Customized Approach Objective	**1.2.2.c** Examine network configuration settings to identify changes made to configurations of NSCs. Interview responsible personnel and examine change control records to verify that identified changes to configurations of NSCs were approved and managed in accordance with Requirement 6.5.1.	
Changes to network connections and NSCs cannot result in misconfiguration, implementation of insecure services, or unauthorized network connections.		
Applicability Notes		
Changes to network connections include the addition, removal, or modification of a connection. Changes to NSC configurations include those related to the component itself as well as those affecting how it performs its security function.		

Exhibit 22A-1

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Maintaining an accurate and up-to-date network diagram(s) prevents network connections and devices from being overlooked and unknowingly left unsecured and vulnerable to compromise. A properly maintained network diagram(s) helps an organization verify its PCI DSS scope by identifying systems connecting to and from the CDE. **Good Practice** All connections to and from the CDE should be identified, including systems providing security, management, or maintenance services to CDE system components. Entities should consider including the following in their network diagrams: • All locations, including retail locations, data centers, corporate locations, cloud providers, etc. • Clear labeling of all network segments. • All security controls providing segmentation, including unique identifiers for each control (for example, name of control, make, model, and version). • All in-scope system components, including NSCs, web app firewalls, anti-malware solutions, change management solutions, IDS/IPS, log aggregation systems, payment terminals, payment applications, HSMs, etc. *(continued on next page)*
1.2.3 An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.	**1.2.3.a** Examine diagram(s) and network configurations to verify that an accurate network diagram(s) exists in accordance with all elements specified in this requirement.	
Customized Approach Objective		
A representation of the boundaries between the CDE, all trusted networks, and all untrusted networks, is maintained and available.	**1.2.3.b** Examine documentation and interview responsible personnel to verify that the network diagram(s) is accurate and updated when there are changes to the environment.	
Applicability Notes		
A current network diagram(s) or other technical or topological solution that identifies network connections and devices can be used to meet this requirement.		

Exhibit 22A-1

Requirements and Testing Procedures		Guidance
1.2.3 *(continued)*		• Clear labeling of any out-of-scope areas on the diagram via a shaded box or other mechanism. • Date of last update, and names of people that made and approved the updates. • A legend or key to explain the diagram. Diagrams should be updated by authorized personnel to ensure diagrams continue to provide an accurate description of the network.
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** An up-to-date, readily available data-flow diagram helps an organization understand and keep track of the scope of its environment by showing how account data flows across networks and between individual systems and devices. Maintaining an up-to-date data-flow diagram(s) prevents account data from being overlooked and unknowingly left unsecured. **Good Practice** The data-flow diagram should include all connection points where account data is received into and sent out of the network, including connections to open, public networks, application processing flows, storage, transmissions between systems and networks, and file backups. *(continued on next page)*
1.2.4 An accurate data-flow diagram(s) is maintained that meets the following: • Shows all account data flows across systems and networks. • Updated as needed upon changes to the environment.	**1.2.4.a** Examine data-flow diagram(s) and interview personnel to verify the diagram(s) show all account data flows in accordance with all elements specified in this requirement. **1.2.4.b** Examine documentation and interview responsible personnel to verify that the data-flow diagram(s) is accurate and updated when there are changes to the environment.	
Customized Approach Objective		
A representation of all transmissions of account data between system components and across network segments is maintained and available.		
Applicability Notes		
A data-flow diagram(s) or other technical or topological solution that identifies flows of account data across systems and networks can be used to meet this requirement.		

Exhibit 22A-1

Requirements and Testing Procedures		Guidance
1.2.4 *(continued)*		The data-flow diagram is meant to be in addition to the network diagram and should reconcile with and augment the network diagram. As a best practice, entities can consider including the following in their data-flow diagrams: • All processing flows of account data, including authorization, capture, settlement, chargeback, and refunds. • All distinct acceptance channels, including card-present, card-not-present, and e-commerce. • All types of data receipt or transmission, including any involving hard copy/paper media. • The flow of account data from the point where it enters the environment, to its final disposition. • Where account data is transmitted and processed, where it is stored, and whether storage is short term or long term. • The source of all account data received (for example, customers, third party, etc.), and any entities with which account data is shared. • Date of last update, and names of people that made and approved the updates.

Exhibit 22A-1

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Compromises often happen due to unused or insecure services (for example, telnet and FTP), protocols, and ports, since these can lead to unnecessary points of access being opened into the CDE. Additionally, services, protocols, and ports that are enabled but not in use are often overlooked and left unsecured and unpatched. By identifying the services, protocols, and ports necessary for business, entities can ensure that all other services, protocols, and ports are disabled or removed. **Good Practice** The security risk associated with each service, protocol, and port allowed should be understood. Approvals should be granted by personnel independent of those managing the configuration. Approving personnel should possess knowledge and accountability appropriate for making approval decisions.
1.2.5 All services, protocols, and ports allowed are identified, approved, and have a defined business need.	**1.2.5.a** Examine documentation to verify that a list exists of all allowed services, protocols, and ports, including business justification and approval for each.	
	1.2.5.b Examine configuration settings for NSCs to verify that only approved services, protocols, and ports are in use.	
Customized Approach Objective		
Unauthorized network traffic (services, protocols, or packets destined for specific ports) cannot enter or leave the network.		

Exhibit 22A-1

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Compromises take advantage of insecure network configurations. **Good Practice** If insecure services, protocols, or ports are necessary for business, the risk posed by these services, protocols, and ports should be clearly understood and accepted by the organization, the use of the service, protocol, or port should be justified, and the security features that mitigate the risk of using these services, protocols, and ports should be defined and implemented by the entity. **Further Information** For guidance on services, protocols, or ports considered to be insecure, refer to industry standards and guidance (for example, from NIST, ENISA, OWASP).
1.2.6 Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.	**1.2.6.a** Examine documentation that identifies all insecure services, protocols, and ports in use to verify that for each, security features are defined to mitigate the risk.	
	1.2.6.b Examine configuration settings for NSCs to verify that the defined security features are implemented for each identified insecure service, protocol, and port.	
Customized Approach Objective		
The specific risks associated with the use of insecure services, protocols, and ports are understood, assessed, and appropriately mitigated.		

Exhibit 22A-1

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Such a review gives the organization an opportunity to clean up any unneeded, outdated, or incorrect rules and configurations which could be utilized by an unauthorized person. Furthermore, it ensures that all rules and configurations allow only authorized services, protocols, and ports that match the documented business justifications. **Good Practice** This review, which can be implemented using manual, automated, or system-based methods, is intended to confirm that the settings that manage traffic rules, what is allowed in and out of the network, match the approved configurations. The review should provide confirmation that all permitted access has a justified business reason. Any discrepancies or uncertainties about a rule or configuration should be escalated for resolution. While this requirement specifies that this review occur at least once every six months, organizations with a high volume of changes to their network configurations may wish to consider performing reviews more frequently to ensure that the configurations continue to meet the needs of the business.
1.2.7 Configurations of NSCs are reviewed at least once every six months to confirm they are relevant and effective.	**1.2.7.a** Examine documentation to verify procedures are defined for reviewing configurations of NSCs at least once every six months.	
	1.2.7.b Examine documentation of reviews of configurations for NSCs and interview responsible personnel to verify that reviews occur at least once every six months.	
Customized Approach Objective	**1.2.7.c** Examine configurations for NSCs to verify that configurations identified as no longer being supported by a business justification are removed or updated.	
NSC configurations that allow or restrict access to trusted networks are verified periodically to ensure that only authorized connections with a current business justification are permitted.		

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** To prevent unauthorized configurations from being applied to the network, stored files with configurations for network controls need to be kept up to date and secured against unauthorized changes. Keeping configuration information current and secure ensures that the correct settings for NSCs are applied whenever the configuration is run. **Examples** If the secure configuration for a router is stored in non-volatile memory, when that router is restarted or rebooted, these controls should ensure that its secure configuration is reinstated.
1.2.8 Configuration files for NSCs are: • Secured from unauthorized access. • Kept consistent with active network configurations.	**1.2.8** Examine configuration files for NSCs to verify they are in accordance with all elements specified in this requirement.	
Customized Approach Objective		
NSCs cannot be defined or modified using untrusted configuration objects (including files).		
Applicability Notes		
Any file or setting used to configure or synchronize NSCs is considered to be a “configuration file.” This includes files, automated and system-based controls, scripts, settings, infrastructure as code, or other parameters that are backed up, archived, or stored remotely.		

Exhibit 22A-1

Requirements and Testing Procedures		Guidance
1.3 Network access to and from the cardholder data environment is restricted.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** This requirement aims to prevent malicious individuals from accessing the entity's network via unauthorized IP addresses or from using services, protocols, or ports in an unauthorized manner. **Good Practice** All traffic inbound to the CDE, regardless of where it originates, should be evaluated to ensure it follows established, authorized rules. Connections should be inspected to ensure traffic is restricted to only authorized communications—for example, by restricting source/destination addresses and ports, and blocking of content. **Examples** Implementing a rule that denies all inbound and outbound traffic that is not specifically needed—for example, by using an explicit "deny all" or implicit deny after allow statement—helps to prevent inadvertent holes that would allow unintended and potentially harmful traffic.
1.3.1 Inbound traffic to the CDE is restricted as follows: • To only traffic that is necessary. • All other traffic is specifically denied.	**1.3.1.a** Examine configuration standards for NSCs to verify that they define restricting inbound traffic to the CDE is in accordance with all elements specified in this requirement.	
	1.3.1.b Examine configurations of NSCs to verify that inbound traffic to the CDE is restricted in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Unauthorized traffic cannot enter the CDE.		

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** This requirement aims to prevent malicious individuals and compromised system components within the entity's network from communicating with an untrusted external host. **Good Practice** All traffic outbound from the CDE, regardless of the destination, should be evaluated to ensure it follows established, authorized rules. Connections should be inspected to restrict traffic to only authorized communications—for example, by restricting source/destination addresses and ports, and blocking of content. **Examples** Implementing a rule that denies all inbound and outbound traffic that is not specifically needed—for example, by using an explicit "deny all" or implicit deny after allow statement—helps to prevent inadvertent holes that would allow unintended and potentially harmful traffic.
1.3.2 Outbound traffic from the CDE is restricted as follows: • To only traffic that is necessary. • All other traffic is specifically denied.	**1.3.2.a** Examine configuration standards for NSCs to verify that they define restricting outbound traffic from the CDE in accordance with all elements specified in this requirement.	
	1.3.2.b Examine configurations of NSCs to verify that outbound traffic from the CDE is restricted in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Unauthorized traffic cannot leave the CDE.		

Exhibit 22A-1

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** The known (or unknown) implementation and exploitation of wireless technology within a network is a common path for malicious individuals to gain access to the network and account data. If a wireless device or network is installed without the entity's knowledge, a malicious individual could easily and "invisibly" enter the network. If NSCs do not restrict access from wireless networks into the CDE, malicious individuals that gain unauthorized access to the wireless network can easily connect to the CDE and compromise account information.
1.3.3 NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: • All wireless traffic from wireless networks into the CDE is denied by default. • Only wireless traffic with an authorized business purpose is allowed into the CDE.	**1.3.3** Examine configuration settings and network diagrams to verify that NSCs are implemented between all wireless networks and the CDE, in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Unauthorized traffic cannot traverse network boundaries between any wireless networks and wired environments in the CDE.		

Requirements and Testing Procedures		Guidance
1.4 Network connections between trusted and untrusted networks are controlled.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Implementing NSCs at every connection coming into and out of trusted networks allows the entity to monitor and control access and minimizes the chances of a malicious individual obtaining access to the internal network via an unprotected connection. **Examples** An entity could implement a DMZ, which is a part of the network that manages connections between an untrusted network (for examples of untrusted networks refer to the Requirement 1 Overview) and services that an organization needs to have available to the public, such as a web server. Please note that if an entity's DMZ processes or transmits account data (for example, e-commerce website), it is also considered a CDE.
1.4.1 NSCs are implemented between trusted and untrusted networks.	**1.4.1.a** Examine configuration standards and network diagrams to verify that NSCs are defined between trusted and untrusted networks.	
	1.4.1.b Examine network configurations to verify that NSCs are in place between trusted and untrusted networks, in accordance with the documented configuration standards and network diagrams.	
Customized Approach Objective		
Unauthorized traffic cannot traverse network boundaries between trusted and untrusted networks.		

Exhibit 22A-1

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Ensuring that public access to a system component is specifically authorized reduces the risk of system components being unnecessarily exposed to untrusted networks. **Good Practice** System components that provide publicly accessible services, such as email, web, and DNS servers, are the most vulnerable to threats originating from untrusted networks. Ideally, such systems are placed within a dedicated trusted network that is public facing (for example, a DMZ) but that is separated via NSCs from more sensitive internal systems, which helps protect the rest of the network in the event these externally accessible systems are compromised. This functionality is intended to prevent malicious actors from accessing the organization's internal network from the Internet, or from using services, protocols, or ports in an unauthorized manner. Where this functionality is provided as a built-in feature of an NSC, the entity should ensure that its configurations do not result in the functionality being disabled or bypassed. **Definitions** Maintaining the "state" (or status) for each connection into a network means the NSC “knows” whether an apparent response to a previous connection is a valid, authorized response (since the NSC retains each connection’s status) or whether it is malicious traffic trying to fool the NSC into allowing the connection.
1.4.2 Inbound traffic from untrusted networks to trusted networks is restricted to: • Communications with system components that are authorized to provide publicly accessible services, protocols, and ports. • Stateful responses to communications initiated by system components in a trusted network. • All other traffic is denied.	**1.4.2** Examine vendor documentation and configurations of NSCs to verify that inbound traffic from untrusted networks to trusted networks is restricted in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Only traffic that is authorized or that is a response to a system component in the trusted network can enter a trusted network from an untrusted network.		
Applicability Notes		
The intent of this requirement is to address communication sessions between trusted and untrusted networks, rather than the specifics of protocols. This requirement does not limit the use of UDP or other connectionless network protocols if state is maintained by the NSC.		

Exhibit 22A-1

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Filtering packets coming into the trusted network helps to, among other things, ensure packets are not “spoofed” to appear as if they are coming from an organization’s own internal network. For example, anti-spoofing measures prevent internal addresses originating from the Internet from passing into the DMZ. **Good Practice** Products usually come with anti-spoofing set as a default and may not be configurable. Entities should consult the vendor's documentation for more information. **Examples** Normally, a packet contains the IP address of the computer that originally sent it so other computers in the network know where the packet originated. Malicious individuals will often try to spoof (or imitate) the sending IP address to fool the target system into believing the packet is from a trusted source.
1.4.3 Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.	**1.4.3** Examine vendor documentation and configurations for NSCs to verify that anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.	
Customized Approach Objective		
Packets with forged IP source addresses cannot enter a trusted network.		

Exhibit 22A-1

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Cardholder data that is directly accessible from an untrusted network, for example, because it is stored on a system within the DMZ or in a cloud database service, is easier for an external attacker to access because there are fewer defensive layers to penetrate. Using NSCs to ensure that system components that store cardholder data (such as a database or a file) can only be directly accessed from trusted networks can prevent unauthorized network traffic from reaching the system component.
1.4.4 System components that store cardholder data are not directly accessible from untrusted networks.	**1.4.4.a** Examine the data-flow diagram and network diagram to verify that it is documented that system components storing cardholder data are not directly accessible from the untrusted networks.	
	1.4.4.b Examine configurations of NSCs to verify that controls are implemented such that system components storing cardholder data are not directly accessible from untrusted networks.	
Customized Approach Objective		
Stored cardholder data cannot be accessed from untrusted networks.		
Applicability Notes		
This requirement is not intended to apply to storage of account data in volatile memory but does apply where memory is being treated as persistent storage (for example, RAM disk). Account data can only be stored in volatile memory during the time necessary to support the associated business process (for example, until completion of the related payment card transaction).		

Exhibit 22A-1

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Restricting the disclosure of internal, private, and local IP addresses is useful to prevent a hacker from obtaining knowledge of these IP addresses and using that information to access the network. **Good Practice** Methods used to meet the intent of this requirement may vary, depending on the specific networking technology being used. For example, the controls used to meet this requirement may be different for IPv4 networks than for IPv6 networks. **Examples** Methods to obscure IP addressing may include, but are not limited to: • IPv4 Network Address Translation (NAT). • Placing system components behind proxy servers/NSCs. • Removal or filtering of route advertisements for internal networks that use registered addressing. • Internal use of RFC 1918 (IPv4) or use IPv6 privacy extension (RFC 4941) when initiating outgoing sessions to the internet.
1.4.5 The disclosure of internal IP addresses and routing information is limited to only authorized parties.	**1.4.5.a** Examine configurations of NSCs to verify that the disclosure of internal IP addresses and routing information is limited to only authorized parties.	
	1.4.5.b Interview personnel and examine documentation to verify that controls are implemented such that any disclosure of internal IP addresses and routing information is limited to only authorized parties.	
Customized Approach Objective		
Internal network information is protected from unauthorized disclosure.		

Exhibit 22A-1

Requirements and Testing Procedures		Guidance
1.5 Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Computing devices that are allowed to connect to the Internet from outside the corporate environment—for example, desktops, laptops, tablets, smartphones, and other mobile computing devices used by employees—are more vulnerable to Internet-based threats. Use of security controls such as host-based controls (for example, personal firewall software or end-point protection solutions), network-based security controls (for example, firewalls, network-based heuristics inspection, and malware simulation), or hardware, helps to protect devices from Internet-based attacks, which could use the device to gain access to the organization's systems and data when the device reconnects to the network. *(continued on next page)*
1.5.1 Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows: • Specific configuration settings are defined to prevent threats being introduced into the entity's network. • Security controls are actively running. • Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period.	**1.5.1.a** Examine policies and configuration standards and interview personnel to verify security controls for computing devices that connect to both untrusted networks, and the CDE, are implemented in accordance with all elements specified in this requirement.	
	1.5.1.b Examine configuration settings on computing devices that connect to both untrusted networks and the CDE to verify settings are implemented in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Devices that connect to untrusted environments and also connect to the CDE cannot introduce threats to the entity's CDE.		

Exhibit 22A-1

Requirements and Testing Procedures		Guidance
Applicability Notes These security controls may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If these security controls need to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period during which these security controls are not active. This requirement applies to employee-owned and company-owned computing devices. Systems that cannot be managed by corporate policy introduce weaknesses and provide opportunities that malicious individuals may exploit.		**Good Practice** The specific configuration settings are determined by the entity and should be consistent with its network security policies and procedures. Where there is a legitimate need to temporarily disable security controls on a company-owned or employee-owned device that connects to both an untrusted network and the CDE—for example, to support a specific maintenance activity or investigation of a technical problem—the reason for taking such action is understood and approved by an appropriate management representative. Any disabling or altering of these security controls, including on administrators' own devices, is performed by authorized personnel. It is recognized that administrators have privileges that may allow them to disable security controls on their own computers, but there should be alerting mechanisms in place when such controls are disabled and follow up that occurs to ensure processes were followed. **Examples** Practices include forbidding split-tunneling of VPNs for employee-owned or corporate-owned mobile devices and requiring that such devices boot up into a VPN.

Exhibit 22A-2

Requirement 2: Apply Secure Configurations to All System Components

Sections

2.1	Processes and mechanisms for applying secure configurations to all system components are defined and understood.
2.2	System components are configured and managed securely.
2.3	Wireless environments are configured and managed securely.

Overview

Malicious individuals, both external and internal to an entity, often use default passwords and other vendor default settings to compromise systems. These passwords and settings are well known and are easily determined via public information.

Applying secure configurations to system components reduces the means available to an attacker to compromise the system. Changing default passwords, removing unnecessary software, functions, and accounts, and disabling or removing unnecessary services all help to reduce the potential attack surface.

Refer to *Appendix G* for definitions of PCI DSS terms.

Exhibit 22A-2

Requirements and Testing Procedures		Guidance
2.1 Processes and mechanisms for applying secure configurations to all system components are defined and understood.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Requirement 2.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 2. While it is important to define the specific policies or procedures called out in Requirement 2, it is equally important to ensure they are properly documented, maintained, and disseminated. **Good Practice** It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle **Definitions** Security policies define the entity's security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives.
2.1.1 All security policies and operational procedures that are identified in Requirement 2 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	**2.1.1** Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 2 are managed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Expectations, controls, and oversight for meeting activities within Requirement 2 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.		

Exhibit 22A-2

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and critical activities may not occur. **Good Practice** Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities. **Examples** A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).
2.1.2 Roles and responsibilities for performing activities in Requirement 2 are documented, assigned, and understood.	**2.1.2.a** Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 2 are documented and assigned.	
Customized Approach Objective	**2.1.2.b** Interview personnel with responsibility for performing activities in Requirement 2 to verify that roles and responsibilities are assigned as documented and are understood.	
Day-to-day responsibilities for performing all the activities in Requirement 2 are allocated. Personnel are accountable for successful, continuous operation of these requirements.		

Exhibit 22A-2

Requirements and Testing Procedures		Guidance
2.2 System components are configured and managed securely.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** There are known weaknesses with many operating systems, databases, network devices, software, applications, container images, and other devices used by an entity or within an entity's environment. There are also known ways to configure these system components to fix security vulnerabilities. Fixing security vulnerabilities reduces the opportunities available to an attacker. By developing standards, entities ensure their system components will be configured consistently and securely and will address the protection of devices for which full hardening may be more difficult. **Good Practice** Keeping up to date with current industry guidance will help the entity maintain secure configurations. The specific controls to be applied to a system will vary and should be appropriate for the type and function of the system. Numerous security organizations have established system-hardening guidelines and recommendations, which advise how to correct common, known weaknesses. **Further Information** Sources for guidance on configuration standards include but are not limited to: Center for Internet Security (CIS), International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Cloud Security Alliance, and product vendors.
2.2.1 Configuration standards are developed, implemented, and maintained to: • Cover all system components. • Address all known security vulnerabilities. • Be consistent with industry-accepted system hardening standards or vendor hardening recommendations. • Be updated as new vulnerability issues are identified, as defined in Requirement 6.3.1. • Be applied when new systems are configured and verified as in place before or immediately after a system component is connected to a production environment.	**2.2.1.a** Examine system configuration standards to verify they define processes that include all elements specified in this requirement. **2.2.1.b** Examine policies and procedures and interview personnel to verify that system configuration standards are updated as new vulnerability issues are identified, as defined in Requirement 6.3.1. **2.2.1.c** Examine configuration settings and interview personnel to verify that system configuration standards are applied when new systems are configured and verified as being in place before or immediately after a system component is connected to a production environment.	
Customized Approach Objective All system components are configured securely and consistently and in accordance with industry-accepted hardening standards or vendor recommendations.		

Exhibit 22A-2

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Malicious individuals often use vendor default account names and passwords to compromise operating systems, applications, and the systems on which they are installed. Because these default settings are often published and are well known, changing these settings will make systems less vulnerable to attack. **Good Practice** All vendor default accounts should be identified, and their purpose and use understood. It is important to establish controls for application and system accounts, including those used to deploy and maintain cloud services so that they do not use default passwords and are not usable by unauthorized individuals. Where a default account is not intended to be used, changing the default password to a unique password that meets PCI DSS Requirement 8.3.6, removing any access to the default account, and then disabling the account, will prevent a malicious individual from re-enabling the account and gaining access with the default password. Using an isolated staging network to install and configure new systems is recommended and can also be used to confirm that default credentials have not been introduced into production environments. **Examples** Defaults to be considered include user IDs, passwords, and other authentication credentials commonly used by vendors in their products.
2.2.2 Vendor default accounts are managed as follows: • If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6. • If the vendor default account(s) will not be used, the account is removed or disabled.	**2.2.2.a** Examine system configuration standards to verify they include managing vendor default accounts in accordance with all elements specified in this requirement.	
	2.2.2.b Examine vendor documentation and observe a system administrator logging on using vendor default accounts to verify accounts are implemented in accordance with all elements specified in this requirement.	
	2.2.2.c Examine configuration files and interview personnel to verify that all vendor default accounts that will not be used are removed or disabled.	
Customized Approach Objective		
System components cannot be accessed using default passwords.		
Applicability Notes		
This applies to ALL vendor default accounts and passwords, including, but not limited to, those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, and Simple Network Management Protocol (SNMP) defaults. This requirement also applies where a system component is not installed within an entity's environment, for example, software and applications that are part of the CDE and are accessed via a cloud subscription service.		

Exhibit 22A-2

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Systems containing a combination of services, protocols, and daemons for their primary function will have a security profile appropriate to allow that function to operate effectively. For example, systems that need to be directly connected to the Internet would have a particular profile, like a DNS server, web server, or an e-commerce server. Conversely, other system components may operate a primary function comprising a different set of services, protocols, and daemons that perform functions that an entity does not want exposed to the Internet. This requirement aims to ensure that different functions do not impact the security profiles of other services in a way which may cause them to operate at a higher or lower security level.
2.2.3 Primary functions requiring different security levels are managed as follows: • Only one primary function exists on a system component, **OR** • Primary functions with differing security levels that exist on the same system component are isolated from each other, **OR** • Primary functions with differing security levels on the same system component are all secured to the level required by the function with the highest security need.	**2.2.3.a** Examine system configuration standards to verify they include managing primary functions requiring different security levels as specified in this requirement. **2.2.3.b** Examine system configurations to verify that primary functions requiring different security levels are managed per one of the ways specified in this requirement. **2.2.3.c** Where virtualization technologies are used, examine the system configurations to verify that system functions requiring different security levels are managed in one of the following ways: • Functions with differing security needs do not co-exist on the same system component. • Functions with differing security needs that exist on the same system component are isolated from each other. • Functions with differing security needs on the same system component are all secured to the level required by the function with the highest security need.	**Good Practice** Ideally, each function should be placed on different system components. This can be achieved by implementing only one primary function on each system component. Another option is to isolate primary functions on the same system component that have different security levels, for example, isolating web servers (which need to be directly connected to the Internet) from application and database servers. *(continued on next page)*
Customized Approach Objective		
Primary functions with lower security needs cannot affect the security of primary functions with higher security needs on the same system component.		

Exhibit 22A-2

Requirements and Testing Procedures		Guidance
2.2.3 *(continued)*		If a system component contains primary functions that need different security levels, a third option is to implement additional controls to ensure that the resultant security level of the primary function(s) with higher security needs is not reduced by the presence of the lower security primary functions. Additionally, the functions with a lower security level should be isolated and/or secured to ensure they cannot access or affect the resources of another system function, and do not introduce security weaknesses to other functions on the same server. Functions of differing security levels may be isolated by either physical or logical controls. For example, a database system should not also be hosting web services unless using controls like virtualization technologies to isolate and contain the functions into separate sub-systems. Another example is using virtual instances or providing dedicated memory access by system function. Where virtualization technologies are used, the security levels should be identified and managed for each virtual component. Examples of considerations for virtualized environments include: • The function of each application, container, or virtual server instance. • How virtual machines (VMs) or containers are stored and secured.

Exhibit 22A-2

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Unnecessary services and functions can provide additional opportunities for malicious individuals to gain access to a system. By removing or disabling all unnecessary services, protocols, daemons, and functions, organizations can focus on securing the functions that are required and reduce the risk that unknown or unnecessary functions will be exploited. **Good Practice** There are many protocols that could be enabled by default that are commonly used by malicious individuals to compromise a network. Disabling or removing all services, functions, and protocols that are not used minimizes the potential attack surface—for example, by removing or disabling an unused FTP or web server. **Examples** Unnecessary functionality may include, but is not limited to scripts, drivers, features, subsystems, file systems, interfaces (USB and Bluetooth), and unnecessary web servers.
2.2.4 Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.	**2.2.4.a** Examine system configuration standards to verify necessary services, protocols, daemons, and functions are identified and documented.	
Customized Approach Objective	**2.2.4.b** Examine system configurations to verify the following: • All unnecessary functionality is removed or disabled. • Only required functionality, as documented in the configuration standards, is enabled.	
System components cannot be compromised by exploiting unnecessary functionality present in the system component.		

Exhibit 22A-2

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Ensuring that all insecure services, protocols, and daemons are adequately secured with appropriate security features makes it more difficult for malicious individuals to exploit common points of compromise within a network. **Good Practice** Enabling security features before new system components are deployed will prevent insecure configurations from being introduced into the environment. Some vendor solutions may provide additional security functions to assist with securing an insecure process. **Further Information** For guidance on services, protocols, or daemons considered to be insecure, refer to industry standards and guidance (for example, as published by NIST, ENISA, and OWASP).
2.2.5 If any insecure services, protocols, or daemons are present: • Business justification is documented. • Additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons.	**2.2.5.a** If any insecure services, protocols, or daemons are present, examine system configuration standards and interview personnel to verify they are managed and implemented in accordance with all elements specified in this requirement.	
Customized Approach Objective	**2.2.5.b** If any insecure services, protocols, or daemons, are present, examine configuration settings to verify that additional security features are implemented to reduce the risk of using insecure services, daemons, and protocols.	
System components cannot be compromised by exploiting insecure services, protocols, or daemons.		

Exhibit 22A-2

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	
2.2.6 System security parameters are configured to prevent misuse.	**2.2.6.a** Examine system configuration standards to verify they include configuring system security parameters to prevent misuse.	**Purpose** Correctly configuring security parameters provided in system components takes advantage of the capabilities of the system component to defeat malicious attacks. **Good Practice** System configuration standards and related processes should specifically address security settings and parameters that have known security implications for each type of system in use. For systems to be configured securely, personnel responsible for configuration and/or administering systems should be knowledgeable in the specific security parameters and settings that apply to the system. Considerations should also include secure settings for parameters used to access cloud portals. **Further Information** Refer to vendor documentation and industry references noted in Requirement 2.2.1 for information about applicable security parameters for each type of system.
	2.2.6.b Interview system administrators and/or security managers to verify they have knowledge of common security parameter settings for system components.	
Customized Approach Objective System components cannot be compromised because of incorrect security parameter configuration.	**2.2.6.c** Examine system configurations to verify that common security parameters are set appropriately and in accordance with the system configuration standards.	

Exhibit 22A-2

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If non-console (including remote) administration does not use encrypted communications, administrative authorization factors (such as IDs and passwords) can be revealed to an eavesdropper. A malicious individual could use this information to access the network, become administrator, and steal data. **Good Practice** Whichever security protocol is used, it should be configured to use only secure versions and configurations to prevent use of an insecure connection—for example, by using only trusted certificates, supporting only strong encryption, and not supporting fallback to weaker, insecure protocols or methods. **Examples** Cleartext protocols (such as HTTP, telnet, etc.) do not encrypt traffic or logon details, making it easy for an eavesdropper to intercept this information. Non-console access may be facilitated by technologies that provide alternative access to systems, including but not limited to, out-of-band (OOB), lights-out management (LOM), Intelligent Platform Management Interface (IPMI), and keyboard, video, mouse (KVM) switches with remote capabilities. These and other non-console access technologies and methods must be secured with strong cryptography. **Further Information** Refer to industry standards and best practices such as *NIST SP 800-52 and SP 800-57*.
2.2.7 All non-console administrative access is encrypted using strong cryptography.	**2.2.7.a** Examine system configuration standards to verify they include encrypting all non-console administrative access using strong cryptography.	
	2.2.7.b Observe an administrator log on to system components and examine system configurations to verify that non-console administrative access is managed in accordance with this requirement.	
	2.2.7.c Examine settings for system components and authentication services to verify that insecure remote login services are not available for non-console administrative access.	
	2.2.7.d Examine vendor documentation and interview personnel to verify that strong cryptography for the technology in use is implemented according to industry best practices and/or vendor recommendations.	
Customized Approach Objective		
Cleartext administrative authorization factors cannot be read or intercepted from any network transmissions.		
Applicability Notes		
This includes administrative access via browser-based interfaces and application programming interfaces (APIs).		

Exhibit 22A-2

<table>
<tr><th colspan="2">Requirements and Testing Procedures</th><th>Guidance</th></tr>
<tr><td colspan="3"><b>2.3 Wireless environments are configured and managed securely.</b></td></tr>
<tr><td><b>Defined Approach Requirements</b></td><td><b>Defined Approach Testing Procedures</b></td><td rowspan="8"><b>Purpose</b>
If wireless networks are not implemented with sufficient security configurations (including changing default settings), wireless sniffers can eavesdrop on the traffic, easily capture data and passwords, and easily enter and attack the network.
<b>Good Practice</b>
Wireless passwords should be constructed so that they are resistant to offline brute force attacks.</td></tr>
<tr><td rowspan="3"><b>2.3.1</b> For wireless environments connected to the CDE or transmitting account data, all wireless vendor defaults are changed at installation or are confirmed to be secure, including but not limited to:
• Default wireless encryption keys.
• Passwords on wireless access points.
• SNMP defaults.
• Any other security-related wireless vendor defaults.</td><td><b>2.3.1.a</b> Examine policies and procedures and interview responsible personnel to verify that processes are defined for wireless vendor defaults to either change them upon installation or to confirm them to be secure in accordance with all elements of this requirement.</td></tr>
<tr><td><b>2.3.1.b</b> Examine vendor documentation and observe a system administrator logging into wireless devices to verify:
• SNMP defaults are not used.
• Default passwords/passphrases on wireless access points are not used.</td></tr>
<tr><td rowspan="5"><b>2.3.1.c</b> Examine vendor documentation and wireless configuration settings to verify other security-related wireless vendor defaults were changed, if applicable.</td></tr>
<tr><td><b>Customized Approach Objective</b></td></tr>
<tr><td>Wireless networks cannot be accessed using vendor default passwords or default configurations.</td></tr>
<tr><td><b>Applicability Notes</b></td></tr>
<tr><td>This includes, but is not limited to, default wireless encryption keys, passwords on wireless access points, SNMP defaults, and any other security-related wireless vendor defaults.</td></tr>
</table>

Exhibit 22A-2

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Changing wireless encryption keys whenever someone with knowledge of the key leaves the organization or moves to a role that no longer requires knowledge of the key, helps keep knowledge of keys limited to only those with a business need to know. Also, changing wireless encryption keys whenever a key is suspected or known to be comprised makes a wireless network more resistant to compromise. **Good Practice** This goal can be accomplished in multiple ways, including periodic changes of keys, changing keys via a defined “joiners-movers-leavers” (JML) process, implementing additional technical controls, and not using fixed pre-shared keys. In addition, any keys that are known to be, or suspected of being, compromised should be managed in accordance with the entity’s incident response plan at Requirement 12.10.1.
2.3.2 For wireless environments connected to the CDE or transmitting account data, wireless encryption keys are changed as follows: • Whenever personnel with knowledge of the key leave the company or the role for which the knowledge was necessary. • Whenever a key is suspected of or known to be compromised.	**2.3.2** Interview responsible personnel and examine key-management documentation to verify that wireless encryption keys are changed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Knowledge of wireless encryption keys cannot allow unauthorized access to wireless networks.		

Exhibit 22A-3

Protect Account Data

Requirement 3: Protect Stored Account Data

Sections

3.1 Processes and mechanisms for protecting stored account data are defined and understood.

3.2 Storage of account data is kept to a minimum.

3.3 Sensitive authentication data (SAD) is not stored after authorization.

3.4 Access to displays of full PAN and ability to copy PAN are restricted.

3.5 Primary account number (PAN) is secured wherever it is stored.

3.6 Cryptographic keys used to protect stored account data are secured.

3.7 Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are defined and implemented.

Overview

Protection methods such as encryption, truncation, masking, and hashing are critical components of account data protection. If an intruder circumvents other security controls and gains access to encrypted account data, the data is unreadable without the proper cryptographic keys and is unusable to that intruder. Other effective methods of protecting stored data should also be considered as potential risk-mitigation opportunities. For example, methods for minimizing risk include not storing account data unless necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies such as e-mail and instant messaging.

If account data is present in non-persistent memory (for example, RAM, volatile memory), encryption of PAN is not required. However, proper controls must be in place to ensure that memory maintains a non-persistent state. Data should be removed from volatile memory once the business purpose (for example, the associated transaction) is complete. In the case that data storage becomes persistent, all applicable PCI DSS Requirements will apply including encryption of stored data.

Requirement 3 applies to protection of stored account data unless specifically called out in an individual requirement.

Refer to *Appendix G* for definitions of “strong cryptography” and other PCI DSS terms.

Requirements and Testing Procedures		Guidance
3.1 Processes and mechanisms for protecting stored account data are defined and understood.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Requirement 3.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 3. While it is important to define the specific policies or procedures called out in Requirement 3, it is equally important to ensure they are properly documented, maintained, and disseminated. **Good Practice** It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle. **Definitions** Security policies define the entity's security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives.
3.1.1 All security policies and operational procedures that are identified in Requirement 3 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	**3.1.1** Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 3 are managed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Expectations, controls, and oversight for meeting activities within Requirement 3 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.		

Exhibit 22A-3

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities, and critical activities may not occur. **Good Practice** Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities. **Examples** A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).
3.1.2 Roles and responsibilities for performing activities in Requirement 3 are documented, assigned, and understood.	**3.1.2.a** Examine documentation to verify that descriptions of roles and responsibilities performing activities in Requirement 3 are documented and assigned.	
	3.1.2.b Interview personnel with responsibility for performing activities in Requirement 3 to verify that roles and responsibilities are assigned as documented and are understood.	
Customized Approach Objective		
Day-to-day responsibilities for performing all the activities in Requirement 3 are allocated. Personnel are accountable for successful, continuous operation of these requirements.		

Exhibit 22A-3

Requirements and Testing Procedures		Guidance
3.2 Storage of account data is kept to a minimum.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** A formal data retention policy identifies what data needs to be retained, for how long, and where that data resides so it can be securely destroyed or deleted as soon as it is no longer needed. The only account data that may be stored after authorization is the primary account number or PAN (rendered unreadable), expiration date, cardholder name, and service code. The storage of SAD data prior to the completion of the authorization process is also included in the data retention and disposal policy so that storage of this sensitive data is kept to minimum, and only retained for the defined amount of time. **Good Practice** When identifying locations of stored account data, consider all processes and personnel with access to the data, as data could have been moved and stored in different locations than originally defined. Storage locations that are often overlooked include backup and archive systems, removable data storage devices, paper-based media, and audio recordings. To define appropriate retention requirements, an entity first needs to understand its own business needs as well as any legal or regulatory obligations that apply to its industry or to the type of data being retained. Implementing an automated process to ensure data is automatically and securely deleted upon its defined retention limit can help ensure that account data is not retained beyond what is necessary for business, legal, or regulatory purposes. *(continued on next page)*
3.2.1 Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following: • Coverage for all locations of stored account data. • Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization. *This bullet is a best practice until its effective date; refer to Applicability Notes below for details.* • Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements. • Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification. • Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy. • A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable.	**3.2.1.a** Examine the data retention and disposal policies, procedures, and processes and interview personnel to verify processes are defined to include all elements specified in this requirement. **3.2.1.b** Examine files and system records on system components where account data is stored to verify that the data storage amount and retention time does not exceed the requirements defined in the data retention policy. **3.2.1.c** Observe the mechanisms used to render account data unrecoverable to verify data cannot be recovered.	
Customized Approach Objective		
Account data is retained only where necessary and for the least amount of time needed and is securely deleted or rendered unrecoverable when no longer needed.		

Exhibit 22A-3

Requirements and Testing Procedures		Guidance
Applicability Notes Where account data is stored by a TPSP (for example, in a cloud environment), entities are responsible for working with their service providers to understand how the TPSP meets this requirement for the entity. Considerations include ensuring that all geographic instances of a data element are securely deleted. *The bullet above (for coverage of SAD stored prior to completion of authorization) is a best practice until 31 March 2025, after which it will be required as part of Requirement 3.2.1 and must be fully considered during a PCI DSS assessment.*		Methods of eliminating data when it exceeds the retention period include secure deletion to complete removal of the data or rendering it unrecoverable and unable to be reconstructed. Identifying and securely eliminating stored data that has exceeded its specified retention period prevents unnecessary retention of data that is no longer needed. This process may be automated, manual, or a combination of both. The deletion function in most operating systems is not “secure deletion” as it allows deleted data to be recovered, so instead, a dedicated secure deletion function or application must be used to make data unrecoverable. *Remember, if you don't need it, don't store it!* **Examples** An automated, programmatic procedure could be run to locate and remove data, or a manual review of data storage areas could be performed. Whichever method is used, it is a good idea to monitor the process to ensure it is completed successfully, and that the results are recorded and validated as being complete. Implementing secure deletion methods ensures that the data cannot be retrieved when it is no longer needed. **Further Information** See *NIST SP 800-88 Rev. 1, Guidelines for Media Sanitization*.

Exhibit 22A-3

Requirements and Testing Procedures		Guidance
3.3 Sensitive authentication data (SAD) is not stored after authorization.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** SAD is very valuable to malicious individuals as it allows them to generate counterfeit payment cards and create fraudulent transactions. Therefore, the storage of SAD upon completion of the authorization process is prohibited. **Good Practice** It may be acceptable for an entity to store SAD in non-persistent memory for a short time after authorization is complete, if following conditions are met: • There is a legitimate business need to access SAD in memory after authorization is complete. • SAD is only ever stored in non-persistent memory (for example, RAM, volatile memory). • Controls are in place to ensure that memory maintains a non-persistent state. • SAD is removed as soon as the business purpose is complete. It is not permissible to store SAD in persistent memory. **Definitions** The authorization process completes when a merchant receives a transaction response (for example, an approval or decline). Refer to *Appendix G* for the definition of "authorization."
3.3.1 SAD is not stored after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process.	**3.3.1.a** If SAD is received, examine documented policies, procedures, and system configurations to verify the data is not stored after authorization.	
	3.3.1.b If SAD is received, examine the documented procedures and observe the secure data deletion processes to verify the data is rendered unrecoverable upon completion of the authorization process.	
Customized Approach Objective		
This requirement is not eligible for the customized approach.		
Applicability Notes		
Issuers and companies that support issuing services, where there is a legitimate and documented business need to store SAD, are not required to meet this requirement. A legitimate business need is one that is necessary for the performance of the function being provided by or for the issuer. Refer to Requirement 3.3.3 for additional requirements specifically for these entities. Sensitive authentication data includes the data cited in Requirements 3.3.1.1 through 3.3.1.3.		

Exhibit 22A-3

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If full contents of any track (from the magnetic stripe on the back of a card if present, equivalent data contained on a chip, or elsewhere) is stored, malicious individuals who obtain that data can use it to reproduce payment cards and complete fraudulent transactions. **Definitions** Full track data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. Each track contains a number of data elements, and this requirement specifies only those that may be retained post-authorization. **Examples** Data sources to review to ensure that the full contents of any track are not retained upon completion of the authorization process include, but are not limited to: • Incoming transaction data. • All logs (for example, transaction, history, debugging, error). • History files. • Trace files. • Database schemas. • Contents of databases, and on-premise and cloud data stores. • Any existing memory/crash dump files.
3.3.1.1 The full contents of any track are not stored upon completion of the authorization process.	**3.3.1.1** Examine data sources to verify that the full contents of any track are not stored upon completion of the authorization process.	
Customized Approach Objective		
This requirement is not eligible for the customized approach.		
Applicability Notes		
In the normal course of business, the following data elements from the track may need to be retained: • Cardholder name. • Primary account number (PAN). • Expiration date. • Service code. To minimize risk, store securely only these data elements as needed for business.		

Exhibit 22A-3

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If card verification code data is stolen, malicious individuals can execute fraudulent Internet and mail-order/telephone-order (MO/TO) transactions. Not storing this data reduces the probability of it being compromised. **Examples** If card verification codes are stored on paper media prior to completion of authorization, a method of erasing or covering the codes should prevent them from being read after authorization is complete. Example methods of rendering the codes unreadable include removing the code with scissors and applying a suitably opaque and un-removable marker over the code. Data sources to review to ensure that the card verification code is not retained upon completion of the authorization process include, but are not limited to: • Incoming transaction data. • All logs (for example, transaction, history, debugging, error). • History files. • Trace files. • Database schemas. • Contents of databases, and on-premise and cloud data stores. • Any existing memory/crash dump files.
3.3.1.2 The card verification code is not stored upon completion of the authorization process.	**3.3.1.2** Examine data sources, to verify that the card verification code is not stored upon completion of the authorization process.	
Customized Approach Objective		
This requirement is not eligible for the customized approach.		
Applicability Notes		
The card verification code is the three- or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions.		

Exhibit 22A-3

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** PIN and PIN blocks should be known only to the card owner or entity that issued the card. If this data is stolen, malicious individuals can execute fraudulent PIN-based transactions (for example, in-store purchases and ATM withdrawals). Not storing this data reduces the probability of it being compromised. **Examples** Data sources to review to ensure that PIN and PIN blocks are not retained upon completion of the authorization process include, but are not limited to: • Incoming transaction data. • All logs (for example, transaction, history, debugging, error). • History files. • Trace files. • Database schemas. • Contents of databases, and on-premise and cloud data stores. • Any existing memory/crash dump files.
3.3.1.3 The personal identification number (PIN) and the PIN block are not stored upon completion of the authorization process.	**3.3.1.3** Examine data sources, to verify that PINs and PIN blocks are not stored upon completion of the authorization process.	
Customized Approach Objective		
This requirement is not eligible for the customized approach.		
Applicability Notes		
PIN blocks are encrypted during the natural course of transaction processes, but even if an entity encrypts the PIN block again, it is still not allowed to be stored after the completion of the authorization process.		

Exhibit 22A-3

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** SAD can be used by malicious individuals to increase the probability of successfully generating counterfeit payment cards and creating fraudulent transactions. **Good Practice** Entities should consider encrypting SAD with a different cryptographic key than is used to encrypt PAN. Note that this does not mean that PAN present in SAD (as part of track data) would need to be separately encrypted.
3.3.2 SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography.	**3.3.2** Examine data stores, system configurations, and/or vendor documentation to verify that all SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography.	
Customized Approach Objective		
This requirement is not eligible for the customized approach. *(continued on next page)*		

Exhibit 22A-3

Requirements and Testing Procedures		Guidance
Applicability Notes Whether SAD is permitted to be stored prior to authorization is determined by the organizations that manage compliance programs (for example, payment brands and acquirers). Contact these organizations for any additional criteria. This requirement applies to all storage of SAD, even if no PAN is present in the environment. Refer to Requirement 3.2.1 for an additional requirement that applies if SAD is stored prior to completion of authorization. Issuers and companies that support issuing services, where there is a legitimate and documented business need to store SAD, are not required to meet this requirement. A legitimate business need is one that is necessary for the performance of the function being provided by or for the issuer. Refer to Requirement 3.3.3 for requirements specifically for these entities. This requirement does not replace how PIN blocks are required to be managed, nor does it mean that a properly encrypted PIN block needs to be encrypted again. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		**Definitions** The authorization process is completed when a merchant receives a transaction response (for example, an approval or decline) . Refer to *Appendix G* for the definition of "authorization."

Exhibit 22A-3

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** SAD can be used by malicious individuals to increase the probability of successfully generating counterfeit payment cards and creating fraudulent transactions**.** **Good Practice** Entities should consider encrypting SAD with a different cryptographic key than is used to encrypt PAN. Note that this does not mean that PAN present in SAD (as part of track data) would need to be separately encrypted.
3.3.3 ***Additional requirement for issuers and companies that support issuing services and store sensitive authentication data:*** Any storage of sensitive authentication data is: • Limited to that which is needed for a legitimate issuing business need and is secured. • Encrypted using strong cryptography. *This bullet is a best practice until its effective date; refer to Applicability Notes below for details.*	**3.3.3.a** ***Additional testing procedure for issuers and companies that support issuing services and store sensitive authentication data:*** Examine documented policies and interview personnel to verify there is a documented business justification for the storage of sensitive authentication data.	
Customized Approach Objective	**3.3.3.b** ***Additional testing procedure for issuers and companies that support issuing services and store sensitive authentication data:*** Examine data stores and system configurations to verify that the sensitive authentication data is stored securely.	
Sensitive authentication data is retained only as required to support issuing functions and is secured from unauthorized access. *(continued on next page)*		

Exhibit 22A-3

Requirements and Testing Procedures		Guidance
Applicability Notes This requirement applies only to issuers and companies that support issuing services and store sensitive authentication data. Entities that issue payment cards or that perform or support issuing services will often create and control sensitive authentication data as part of the issuing function. It is allowable for companies that perform, facilitate, or support issuing services to store sensitive authentication data ONLY IF they have a legitimate business need to store such data. A legitimate issuing business need is one that is necessary for the performance of the function being provided by or for the issuer. *The bullet above (for encrypting stored SAD with strong cryptography) is a best practice until 31 March 2025, after which it will be required as part of Requirement 3.3.3 and must be fully considered during a PCI DSS assessment.*		

Exhibit 22A-3

Requirements and Testing Procedures		Guidance
3.4 Access to displays of full PAN and ability to copy PAN are restricted.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** The display of full PAN on computer screens, payment card receipts, paper reports, etc. can result in this data being obtained by unauthorized individuals and used fraudulently. Ensuring that the full PAN is displayed only for those with a legitimate business need minimizes the risk of unauthorized persons gaining access to PAN data. **Good Practice** Applying access controls according to defined roles is one way to limit access to viewing full PAN to only those individuals with a defined business need. The masking approach should always display only the number of digits needed to perform a specific business function. For example, if only the last four digits are needed to perform a business function, PAN should be masked to only show the last four digits. As another example, if a function needs to view the bank identification number (BIN) for routing purposes, unmask only the BIN digits for that function. *(continued on next page)*
3.4.1 PAN is masked when displayed (the BIN and last four digits **are the maximum number** of digits to be displayed), such that only personnel with a legitimate business need can see **more than** the BIN and last four digits of the PAN. *(continued on next page)*	**3.4.1.a** Examine documented policies and procedures for masking the display of PANs to verify: • A list of roles that need access to more than the BIN and last four digits of the PAN (includes full PAN) is documented, together with a legitimate business need for each role to have such access. • PAN is masked when displayed such that only personnel with a legitimate business need can see more than the BIN and last four digits of the PAN. • All roles not specifically authorized to see the full PAN must only see masked PANs.	
	3.4.1.b Examine system configurations to verify that full PAN is only displayed for roles with a documented business need, and that PAN is masked for all other requests.	
	3.4.1.c Examine displays of PAN (for example, on screen, on paper receipts) to verify that PANs are masked when displayed, and that only those with a legitimate business need are able to see more than the BIN and/or last four digits of the PAN.	

Exhibit 22A-3

Requirements and Testing Procedures		Guidance
Customized Approach Objective PAN displays are restricted to the minimum number of digits necessary to meet a defined business need.		**Definitions** Masking is not synonymous with truncation and these terms cannot be used interchangeably. Masking refers to the concealment of certain digits during display or printing, even when the entire PAN is stored on a system. This is different from truncation, in which the truncated digits are removed and cannot be retrieved within the system. Masked PAN could be “unmasked”, but there is no "un-truncation" without recreating the PAN from another source. Refer to *Appendix G* for definitions of “masking” and “truncation.” **Further Information** For more information about masking and truncation, see PCI SSC’s FAQs on these topics.
Applicability Notes This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment brand requirements for point-of-sale (POS) receipts. This requirement relates to protection of PAN where it is displayed on screens, paper receipts, printouts, etc., and is not to be confused with Requirement 3.5.1 for protection of PAN when stored, processed, or transmitted.		

Exhibit 22A-3

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Relocation of PAN to unauthorized storage devices is a common way for this data to be obtained and used fraudulently. Methods to ensure that only those with explicit authorization and a legitimate business reason can copy or relocate PAN minimizes the risk of unauthorized persons gaining access to PAN. **Good Practice** Copying and relocation of PAN should only be done to storage devices that are permissible and authorized for that individual. **Definitions** A virtual desktop is an example of a remote-access technology. Such remote access technologies often include tools to disable copy and/or relocation functionality. Storage devices include, but are not limited to, local hard drives, virtual drives, removable electronic media, network drives, and cloud storage. **Further Information** Vendor documentation for the remote-access technology in use will provide information about the system settings needed to implement this requirement.
3.4.2 When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need. **Customized Approach Objective** PAN cannot be copied or relocated by unauthorized personnel using remote-access technologies.	**3.4.2.a** Examine documented policies and procedures and documented evidence for technical controls that prevent copy and/or relocation of PAN when using remote-access technologies onto local hard drives or removable electronic media to verify the following: • Technical controls prevent all personnel not specifically authorized from copying and/or relocating PAN. • A list of personnel with permission to copy and/or relocate PAN is maintained, together with the documented, explicit authorization and legitimate, defined business need.	
Applicability Notes Storing or relocating PAN onto local hard drives, removable electronic media, and other storage devices brings these devices into scope for PCI DSS. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	**3.4.2.b** Examine configurations for remote-access technologies to verify that technical controls to prevent copy and/or relocation of PAN for all personnel, unless explicitly authorized. **3.4.2.c** Observe processes and interview personnel to verify that only personnel with documented, explicit authorization and a legitimate, defined business need have permission to copy and/or relocate PAN when using remote-access technologies.	

Exhibit 22A-3

Requirements and Testing Procedures		Guidance
3.5 Primary account number (PAN) is secured wherever it is stored.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Rendering stored PAN unreadable is a defense in depth control designed to protect the data if an unauthorized individual gains access to stored data by taking advantage of a vulnerability or misconfiguration of an entity's primary access control. **Good Practice** It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed versions of a PAN. Controls that prevent the correlation of this data will help ensure that the original PAN remains unreadable. Implementing keyed cryptographic hashes with associated key management processes and procedures in accordance with Requirement 3.5.1.1 is a valid additional control to prevent correlation. **Further Information** For information about truncation formats and truncation in general, see PCI SSC's FAQs on the topic. Sources for information about index tokens include: • PCI SSC's Tokenization Product Security Guidelines (*https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf*) • *ANSI X9.119-2-2017: Retail Financial Services - Requirements For Protection Of Sensitive Payment Card Data - Part 2: Implementing Post-Authorization Tokenization Systems*
3.5.1 PAN is rendered unreadable anywhere it is stored by using any of the following approaches: • One-way hashes based on strong cryptography of the entire PAN. • Truncation (hashing cannot be used to replace the truncated segment of PAN). – If hashed and truncated versions of the same PAN, or different truncation formats of the same PAN, are present in an environment, additional controls are in place such that the different versions cannot be correlated to reconstruct the original PAN. • Index tokens. • Strong cryptography with associated key-management processes and procedures.	**3.5.1.a** Examine documentation about the system used to render PAN unreadable, including the vendor, type of system/process, and the encryption algorithms (if applicable) to verify that the PAN is rendered unreadable using any of the methods specified in this requirement. **3.5.1.b** Examine data repositories and audit logs, including payment application logs, to verify the PAN is rendered unreadable using any of the methods specified in this requirement. **3.5.1.c** If hashed and truncated versions of the same PAN are present in the environment, examine implemented controls to verify that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.	
Customized Approach Objective		
Cleartext PAN cannot be read from storage media.		
Applicability Notes		
This requirement applies to PANs stored in primary storage (databases, or flat files such as text files spreadsheets) as well as non-primary storage (backup, audit logs, exception, or troubleshooting logs). This requirement does not preclude the use of temporary files containing cleartext PAN while encrypting and decrypting PAN.		

Exhibit 22A-3

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Rendering stored PAN unreadable is a defense in depth control designed to protect the data if an unauthorized individual gains access to stored data by taking advantage of a vulnerability or misconfiguration of an entity's primary access control. A hashing function that incorporates a randomly generated secret key provides brute force attack resistance and secret authentication integrity. **Definitions** Refer to *Appendix G* for the definition of "keyed cryptographic hash" and for information about appropriate keyed cryptographic hashing algorithms and additional resources. **Examples** Systems which only have access to one hash value at a time and which store no other account data on the same system as the hash, are not required to meet key-management processes and procedures (Requirements 3.6 and 3.7). Examples of such systems include transaction-originating devices that generate a hash of the PAN for use in a backend system, such as pay-at-gate transit turnstiles. However, in such an implementation, the backend system will have access to more than one hash value at a time, and therefore is required to meet key-management processes and procedures at Requirements 3.6 and 3.7.
3.5.1.1 Hashes used to render PAN unreadable (per the first bullet of Requirement 3.5.1) are keyed cryptographic hashes of the entire PAN, with associated key-management processes and procedures in accordance with Requirements 3.6 and 3.7.	**3.5.1.1.a** Examine documentation about the hashing method used to render PAN unreadable, including the vendor, type of system/process, and the encryption algorithms (as applicable) to verify that the hashing method results in keyed cryptographic hashes of the entire PAN, with associated key management processes and procedures.	
Customized Approach Objective		
Cleartext PAN cannot be determined from hashes of the PAN.	**3.5.1.1.b** Examine documentation about the key management procedures and processes associated with the keyed cryptographic hashes to verify keys are managed in accordance with Requirements 3.6 and 3.7.	
	3.5.1.1.c Examine data repositories to verify the PAN is rendered unreadable.	
	3.5.1.1.d Examine audit logs, including payment application logs, to verify the PAN is rendered unreadable.	
Applicability Notes		
All Applicability Notes for Requirement 3.5.1 also apply to this requirement. *(continued on next page)*		

Exhibit 22A-3

Requirements and Testing Procedures		Guidance
(continued) Key-management processes and procedures (Requirements 3.6 and 3.7) do not apply to system components used to generate individual keyed hashes of a PAN for comparison to another system if: • The system components only have access to one hash value at a time (hash values are not stored on the system) **AND** • There is no other account data stored on the same system as the hashes. *This requirement is considered a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment. This requirement will replace the bullet in Requirement 3.5.1 for one-way hashes once its effective date is reached.*		

Exhibit 22A-3

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Disk-level and partition-level encryption typically encrypts the entire disk or partition using the same key, with all data automatically decrypted when the system runs or when an authorized user requests it. For this reason, disk-level encryption is not appropriate to protect stored PAN on computers, laptops, servers, storage arrays, or any other system that provides transparent decryption upon user authentication. **Further Information** Where available, following vendors' hardening and industry best practice guidelines can assist in securing PAN on these devices.
3.5.1.2 If disk-level or partition-level encryption (rather than file-, column-, or field-level database encryption) is used to render PAN unreadable, it is implemented only as follows: • On removable electronic media **OR** • If used for non-removable electronic media, PAN is also rendered unreadable via another mechanism that meets Requirement 3.5.1.	**3.5.1.2.a** Examine encryption processes to verify that, if disk-level or partition-level encryption is used to render PAN unreadable, it is implemented only as follows: • On removable electronic media, **OR** • If used for non-removable electronic media, examine encryption processes used to verify that PAN is also rendered unreadable via another method that meets Requirement 3.5.1.	
Customized Approach Objective	**3.5.1.2.b** Examine configurations and/or vendor documentation and observe encryption processes to verify the system is configured according to vendor documentation the result is that the disk or the partition is rendered unreadable.	
Encrypted PAN is only decrypted when there is a legitimate business need to access that PAN. *(continued on next page)*		

Exhibit 22A-3

Requirements and Testing Procedures		Guidance
Applicability Notes *(continued)* This requirement applies to any encryption method that provides clear-text PAN automatically when a system runs, even though an authorized user has not specifically requested that data. While disk or partition encryption may still be present on these types of devices, it cannot be the only mechanism used to protect PAN stored on those systems. Any stored PAN must also be rendered unreadable per Requirement 3.5.1—for example, through truncation or a data-level encryption mechanism. Full disk encryption helps to protect data in the event of physical loss of a disk and therefore its use is appropriate only for removable electronic media storage devices. Media that is part of a data center architecture (for example, hot-swappable drives, bulk tape-backups) is considered non-removable electronic media to which Requirement 3.5.1 applies. Disk or partition encryption implementations must also meet all other PCI DSS encryption and key-management requirements. For issuers and companies that support issuing services: This requirement does not apply to PANs being accessed for real-time transaction processing. However, it does apply to PANs stored for other purposes. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

Exhibit 22A-3

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Disk-level encryption typically encrypts the entire disk or partition using the same key, with all data automatically decrypted when the system runs or when an authorized user requests it. Many disk-encryption solutions intercept operating system read/write operations and perform the appropriate cryptographic transformations without any special action by the user other than supplying a password or passphrase at system start-up or at the beginning of a session. This provides no protection from a malicious individual that has already managed to gain access to a valid user account. **Good Practice** Full disk encryption helps to protect data in the event of physical loss of a disk and therefore its use is best limited only to removable electronic media storage devices.
3.5.1.3 If disk-level or partition-level encryption is used (rather than file-, column-, or field-level database encryption) to render PAN unreadable, it is managed as follows: • Logical access is managed separately and independently of native operating system authentication and access control mechanisms. • Decryption keys are not associated with user accounts. • Authentication factors (passwords, passphrases, or cryptographic keys) that allow access to unencrypted data are stored securely.	**3.5.1.3.a** If disk-level or partition-level encryption is used to render PAN unreadable, examine the system configuration and observe the authentication process to verify that logical access is implemented in accordance with all elements specified in this requirement. **3.5.1.3.b** Examine files containing authentication factors (passwords, passphrases, or cryptographic keys) and interview personnel to verify that authentication factors that allow access to unencrypted data are stored securely and are independent from the native operating system's authentication and access control methods.	
Customized Approach Objective		
Disk encryption implementations are configured to require independent authentication and logical access controls for decryption.		
Applicability Notes		
Disk or partition encryption implementations must also meet all other PCI DSS encryption and key-management requirements.		

Requirements and Testing Procedures		Guidance
3.6 Cryptographic keys used to protect stored account data are secured.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Cryptographic keys must be strongly protected because those who obtain access will be able to decrypt data. **Good Practice** Having a centralized key management system based on industry standards is recommended for managing cryptographic keys. **Further Information** The entity's key management procedures will benefit through alignment with industry requirements, Sources for information on cryptographic key management life cycles include: • *ISO 11568-1 Banking — Key management (retail) — Part 1*: Principles (specifically Chapter 10 and the referenced Parts 2 & 4) • *NIST SP 800-57 Part 1 Revision 5—Recommendation for Key Management, Part 1: General*.
3.6.1 Procedures are defined and implemented to protect cryptographic keys used to protect stored account data against disclosure and misuse that include: • Access to keys is restricted to the fewest number of custodians necessary. • Key-encrypting keys are at least as strong as the data-encrypting keys they protect. • Key-encrypting keys are stored separately from data-encrypting keys. • Keys are stored securely in the fewest possible locations and forms.	**3.6.1** Examine documented key-management policies and procedures to verify that processes to protect cryptographic keys used to protect stored account data against disclosure and misuse are defined to include all elements specified in this requirement.	
Customized Approach Objective		
Processes that protect cryptographic keys used to protect stored account data against disclosure and misuse are defined and implemented.		
Applicability Notes		
This requirement applies to keys used to protect stored account data and to key-encrypting keys used to protect data-encrypting keys. The requirement to protect keys used to protect stored account data from disclosure and misuse applies to both data-encrypting keys and key-encrypting keys. Because one key-encrypting key may grant access to many data-encrypting keys, the key-encrypting keys require strong protection measures.		

Exhibit 22A-3

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Maintaining current documentation of the cryptographic architecture enables an entity to understand the algorithms, protocols, and cryptographic keys used to protect stored account data, as well as the devices that generate, use, and protect the keys. This allows an entity to keep pace with evolving threats to its architecture and plan for updates as the assurance level provided by different algorithms and key strengths changes. Maintaining such documentation also allows an entity to detect lost or missing keys or key-management devices and identify unauthorized additions to its cryptographic architecture. The use of the same cryptographic keys in both production and test environments introduces a risk of exposing the key if the test environment is not at the same security level as the production environment. **Good Practice** Having an automated reporting mechanism can assist with maintenance of the cryptographic attributes.
3.6.1.1 ***Additional requirement for service providers only:*** A documented description of the cryptographic architecture is maintained that includes: • Details of all algorithms, protocols, and keys used for the protection of stored account data, including key strength and expiry date. • Preventing the use of the same cryptographic keys in production and test environments. *This bullet is a best practice until its effective date; refer to Applicability Notes below for details.* • Description of the key usage for each key. • Inventory of any hardware security modules (HSMs), key management systems (KMS), and other secure cryptographic devices (SCDs) used for key management, including type and location of devices, to support meeting Requirement 12.3.4.	**3.6.1.1** ***Additional testing procedure for service provider assessments only:*** Interview responsible personnel and examine documentation to verify that a document exists to describe the cryptographic architecture that includes all elements specified in this requirement.	
Customized Approach Objective		
Accurate details of the cryptographic architecture are maintained and available. *(continued on next page)*		

Exhibit 22A-3

Requirements and Testing Procedures		Guidance
Applicability Notes		
This requirement applies only when the entity being assessed is a service provider. In cloud HSM implementations, responsibility for the cryptographic architecture according to this Requirement will be shared between the cloud provider and the cloud customer. *The bullet above (for including, in the cryptographic architecture, that the use of the same cryptographic keys in production and test is prevented) is a best practice until 31 March 2025, after which it will be required as part of Requirement 3.6.1.1 and must be fully considered during a PCI DSS assessment.*		

Exhibit 22A-3

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Storing cryptographic keys securely prevents unauthorized or unnecessary access that could result in the exposure of stored account data. Storing keys separately means they are stored such that if the location of one key is compromised, the second key is not also compromised. **Good Practice** Where data-encrypting keys are stored in an HSM, the HSM interaction channel should be protected to prevent interception of encryption or decryption operations.
3.6.1.2 Secret and private keys used to protect stored account data are stored in one (or more) of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. • Within a secure cryptographic device (SCD), such as a hardware security module (HSM) or PTS-approved point-of-interaction device. • As at least two full-length key components or key shares, in accordance with an industry-accepted method.	**3.6.1.2.a** Examine documented procedures to verify it is defined that cryptographic keys used to encrypt/decrypt stored account data must exist only in one (or more) of the forms specified in this requirement.	
	3.6.1.2.b Examine system configurations and key storage locations to verify that cryptographic keys used to encrypt/decrypt stored account data exist in one (or more) of the forms specified in this requirement.	
	3.6.1.2.c Wherever key-encrypting keys are used, examine system configurations and key storage locations to verify: • Key-encrypting keys are at least as strong as the data-encrypting keys they protect. • Key-encrypting keys are stored separately from data-encrypting keys.	
Customized Approach Objective		
Secret and private keys are stored in a secure form that prevents unauthorized retrieval or access. *(continued on next page)*		

Exhibit 22A-3

Requirements and Testing Procedures		Guidance
Applicability Notes		
It is not required that public keys be stored in one of these forms. Cryptographic keys stored as part of a key management system (KMS) that employs SCDs are acceptable. A cryptographic key that is split into two parts does not meet this requirement. Secret or private keys stored as key components or key shares must be generated via one of the following: • Using an approved random number generator and within an SCD, **OR** • According to ISO 19592 or equivalent industry standard for generation of secret key shares.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Restricting the number of people who have access to cleartext cryptographic key components reduces the risk of stored account data being retrieved or rendered visible by unauthorized parties. **Good Practice** Only personnel with defined key custodian responsibilities (creating, altering, rotating, distributing, or otherwise maintaining encryption keys) should be granted access to key components. Ideally this will be a very small number of people.
3.6.1.3 Access to cleartext cryptographic key components is restricted to the fewest number of custodians necessary.	**3.6.1.3** Examine user access lists to verify that access to cleartext cryptographic key components is restricted to the fewest number of custodians necessary.	
Customized Approach Objective		
Access to cleartext cryptographic key components is restricted to necessary personnel.		

Exhibit 22A-3

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Storing any cryptographic keys in the fewest locations helps an organization track and monitor all key locations and minimizes the potential for keys to be exposed to unauthorized parties.
3.6.1.4 Cryptographic keys are stored in the fewest possible locations.	**3.6.1.4** Examine key storage locations and observe processes to verify that keys are stored in the fewest possible locations.	
Customized Approach Objective		
Cryptographic keys are retained only where necessary.		

Exhibit 22A-3

Requirements and Testing Procedures		Guidance
3.7 Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are defined and implemented.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Use of strong cryptographic keys significantly increases the level of security of encrypted account data. **Further Information** See the sources referenced at Cryptographic Key Generation in *Appendix G*.
3.7.1 Key-management policies and procedures are implemented to include generation of strong cryptographic keys used to protect stored account data.	**3.7.1.a** Examine the documented key-management policies and procedures for keys used for protection of stored account data to verify that they define generation of strong cryptographic keys.	
	3.7.1.b Observe the method for generating keys to verify that strong keys are generated.	
Customized Approach Objective		
Strong cryptographic keys are generated.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Secure distribution or conveyance of secret or private cryptographic keys means that keys are distributed only to authorized custodians, as identified in Requirement 3.6.1.2, and are never distributed insecurely.
3.7.2 Key-management policies and procedures are implemented to include secure distribution of cryptographic keys used to protect stored account data.	**3.7.2.a** Examine the documented key-management policies and procedures for keys used for protection of stored account data to verify that they define secure distribution of cryptographic keys.	
	3.7.2.b Observe the method for distributing keys to verify that keys are distributed securely.	
Customized Approach Objective		
Cryptographic keys are secured during distribution.		

Exhibit 22A-3

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Storing keys without proper protection could provide access to attackers, resulting in the decryption and exposure of account data. **Good Practice** Data encryption keys can be protected by encrypting them with a key-encrypting key. Keys can be stored in a Hardware Security Module (HSM). Secret or private keys that can decrypt data should never be present in source code.
3.7.3 Key-management policies and procedures are implemented to include secure storage of cryptographic keys used to protect stored account data.	**3.7.3.a** Examine the documented key-management policies and procedures for keys used for protection of stored account data to verify that they define secure storage of cryptographic keys. **3.7.3.b** Observe the method for storing keys to verify that keys are stored securely.	
Customized Approach Objective		
Cryptographic keys are secured when stored.		

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	
3.7.4 Key management policies and procedures are implemented for cryptographic key changes for keys that have reached the end of their cryptoperiod, as defined by the associated application vendor or key owner, and based on industry best practices and guidelines, including the following: • A defined cryptoperiod for each key type in use. • A process for key changes at the end of the defined cryptoperiod.	**3.7.4.a** Examine the documented key-management policies and procedures for keys used for protection of stored account data to verify that they define changes to cryptographic keys that have reached the end of their cryptoperiod and include all elements specified in this requirement.	**Purpose** Changing encryption keys when they reach the end of their cryptoperiod is imperative to minimize the risk of someone obtaining the encryption keys and using them to decrypt data. **Definitions** A cryptoperiod is the time span during which a cryptographic key can be used for its defined purpose. Cryptoperiods are often defined in terms of the period for which the key is active and/or the amount of cipher-text that has been produced by the key. Considerations for defining the cryptoperiod include, but are not limited to, the strength of the underlying algorithm, size or length of the key, risk of key compromise, and the sensitivity of the data being encrypted. **Further Information** *NIST SP 800-57 Part 1, Revision 5, Section 5.3 Cryptoperiods* – provides guidance for establishing the time span during which a specific key is authorized for use by legitimate entities, or the keys for a given system will remain in effect. See Table 1 of *SP 800-57* Part 1 for suggested cryptoperiods for different key types.
	3.7.4.b Interview personnel, examine documentation, and observe key storage locations to verify that keys are changed at the end of the defined cryptoperiod(s).	
Customized Approach Objective		
Cryptographic keys are not used beyond their defined cryptoperiod.		

Exhibit 22A-3

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Keys that are no longer required, keys with weakened integrity, and keys that are known or suspected to be compromised, should be archived, revoked, and/or destroyed to ensure that the keys can no longer be used. If such keys need to be kept (for example, to support archived encrypted data), they should be strongly protected. **Good Practice** Archived cryptographic keys should be used only for decryption/verification purposes. The encryption solution should provide for and facilitate a process to replace keys that are due for replacement or that are known to be, or suspected of being, compromised. In addition, any keys that are known to be, or suspected of being, compromised should be managed in accordance with the entity's incident response plan per Requirement 12.10.1. **Further Information** Industry best practices for archiving retired keys are outlined in *NIST SP 800-57 Part 1, Revision 5, Section 8.3.1*, and includes maintaining the archive with a trusted third party and storing archived key information separately from operational data.
3.7.5 Key management policies procedures are implemented to include the retirement, replacement, or destruction of keys used to protect stored account data, as deemed necessary when: • The key has reached the end of its defined cryptoperiod. • The integrity of the key has been weakened, including when personnel with knowledge of a cleartext key component leaves the company, or the role for which the key component was known. • The key is suspected of or known to be compromised. Retired or replaced keys are not used for encryption operations.	**3.7.5.a** Examine the documented key-management policies and procedures for keys used for protection of stored account data and verify that they define retirement, replacement, or destruction of keys in accordance with all elements specified in this requirement. **3.7.5.b** Interview personnel to verify that processes are implemented in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Keys are removed from active use when it is suspected or known that the integrity of the key is weakened.		
Applicability Notes		
If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key).		

Exhibit 22A-3

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Split knowledge and dual control of keys are used to eliminate the possibility of a single person having access to the whole key and therefore being able to gain unauthorized access to the data. **Definitions** Split knowledge is a method in which two or more people separately have key components, where each person knows only their own key component, and the individual key components convey no knowledge of other components or of the original cryptographic key. Dual control requires two or more people to authenticate the use of a cryptographic key or perform a key-management function. No single person can access or use the authentication factor (for example, the password, PIN, or key) of another. **Good Practice** Where key components or key shares are used, procedures should ensure that no single custodian ever has access to sufficient key components or shares to reconstruct the cryptographic key. For example, in an m-of-n scheme (for example, Shamir), where only two of any three components are required to reconstruct the cryptographic key, a custodian must not have current or prior knowledge of more than one component. If a custodian was previously assigned component A, which was then reassigned, the custodian should not then be assigned component B or C, as this would give the custodian knowledge of two components and the ability to recreate the key. *(continued on next page)*
3.7.6 Where manual cleartext cryptographic key-management operations are performed by personnel, key-management policies and procedures are implemented, including managing these operations using split knowledge and dual control.	**3.7.6.a** Examine the documented key-management policies and procedures for keys used for protection of stored account data and verify that they define using split knowledge and dual control. **3.7.6.b** Interview personnel and/or observe processes to verify that manual cleartext keys are managed with split knowledge and dual control.	
Customized Approach Objective		
Cleartext secret or private keys cannot be known by anyone. Operations involving cleartext keys cannot be carried out by a single person.		
Applicability Notes		
This control is applicable for manual key-management operations. A cryptographic key that is simply split into two parts does not meet this requirement. Secret or private keys stored as key components or key shares must be generated via one of the following: • Using an approved random number generator and within a secure cryptographic device (SCD), such as a hardware security module (HSM) or PTS-approved point-of-interaction device, **OR** • According to ISO 19592 or equivalent industry standard for generation of secret key shares.		

Exhibit 22A-3

Requirements and Testing Procedures		Guidance
3.7.6 *(continued)*		**Examples** Key-management operations that might be performed manually include, but are not limited to, key generation, transmission, loading, storage, and destruction. **Further Information** Industry standards for managing key components include: • *NIST SP 800-57* Part 2, Revision 1 -- Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations [4.6 Keying Material Distribution] • *ISO 11568-2 Banking — Key management (retail) — Part 2*: Symmetric ciphers, their key management and life cycle [4.7.2.3 Key components and 4.9.3 Key components] • *European Payments Council EPC342-08 Guidelines on Cryptographic Algorithms Usage and Key Management* [especially 4.1.4 Key installation].
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If an attacker is able to substitute an entity's key with a key the attacker knows, the attacker will be able to decrypt all data encrypted with that key. **Good Practice** The encryption solution should not allow for or accept substitution of keys from unauthorized sources or unexpected processes. Controls should include ensuring that individuals with access to key components or shares do not have access to other components or shares that form the necessary threshold to derive the key.
3.7.7 Key management policies and procedures are implemented to include the prevention of unauthorized substitution of cryptographic keys.	**3.7.7.a** Examine the documented key-management policies and procedures for keys used for protection of stored account data and verify that they define prevention of unauthorized substitution of cryptographic keys. **3.7.7.b** Interview personnel and/or observe processes to verify that unauthorized substitution of keys is prevented.	
Customized Approach Objective		
Cryptographic keys cannot be substituted by unauthorized personnel.		

Exhibit 22A-3

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** This process will help ensure individuals that act as key custodians commit to the key-custodian role and understand and accept the responsibilities. An annual reaffirmation can help remind key custodians of their responsibilities. **Further Information** Industry guidance for key custodians and their roles and responsibilities includes: • *NIST SP 800-130 A Framework for Designing Cryptographic Key Management Systems* [5. Roles and Responsibilities (especially) for Key Custodians] • *ISO 11568-1 Banking -- Key management (retail) -- Part 1*: Principles [5 Principles of key management (especially b)]
3.7.8 Key management policies and procedures are implemented to include that cryptographic key custodians formally acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities.	**3.7.8.a** Examine the documented key-management policies and procedures for keys used for protection of stored account data and verify that they define acknowledgments for key custodians in accordance with all elements specified in this requirement.	
	3.7.8.b Examine documentation or other evidence showing that key custodians have provided acknowledgments in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Key custodians are knowledgeable about their responsibilities in relation to cryptographic operations and can access assistance and guidance when required.		

Exhibit 22A-3

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Providing guidance to customers on how to securely transmit, store, and update cryptographic keys can help prevent keys from being mismanaged or disclosed to unauthorized entities. **Further Information** Numerous industry standards for key management are cited above in the Guidance for Requirements 3.7.1-3.7.8.
3.7.9 *Additional requirement for service providers only:* Where a service provider shares cryptographic keys with its customers for transmission or storage of account data, guidance on secure transmission, storage and updating of such keys is documented and distributed to the service provider's customers.	**3.7.9 *Additional testing procedure for service provider assessments only:*** If the service provider shares cryptographic keys with its customers for transmission or storage of account data, examine the documentation that the service provider provides to its customers to verify it includes guidance on how to securely transmit, store, and update customers' keys in accordance with all elements specified in Requirements 3.7.1 through 3.7.8 above.	
Customized Approach Objective		
Customers are provided with appropriate key management guidance whenever they receive shared cryptographic keys.		
Applicability Notes		
This requirement applies only when the entity being assessed is a service provider.		

Exhibit 22A-4

Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks

Sections

4.1 Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and understood.

4.2 PAN is protected with strong cryptography during transmission

Overview

The use of strong cryptography provides greater assurance in preserving data confidentiality, integrity, and non-repudiation.

To protect against compromise, PAN must be encrypted during transmission over networks that are easily accessed by malicious individuals, including untrusted and public networks. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targeted by malicious individuals aiming to exploit these vulnerabilities to gain privileged access to cardholder data environments (CDE). Any transmissions of cardholder data over an entity's internal network(s) will naturally bring that network into scope for PCI DSS since that network stores, processes, or transmits cardholder data. Any such networks must be evaluated and assessed against applicable PCI DSS requirements.

Requirement 4 applies to transmissions of PAN unless specifically called out in an individual requirement.

PAN transmissions can be protected by encrypting the data before it is transmitted, or by encrypting the session over which the data is transmitted, or both. While it is not required that strong cryptography be applied at both the data level and the session level, it is recommended.

Refer to *Appendix G* for definitions of "strong cryptography" and other PCI DSS terms.

Exhibit 22A-4

Requirements and Testing Procedures		Guidance
4.1 Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and understood.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Requirement 4.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 4. While it is important to define the specific policies or procedures called out in Requirement 4, it is equally important to ensure they are properly documented, maintained, and disseminated. **Good Practice** It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle. **Definitions** Security policies define the entity's security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives. Policies and procedures, including updates, are actively communicated to all affected personnel, and are supported by operating procedures describing how to perform activities.
4.1.1 All security policies and operational procedures that are identified in Requirement 4 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	**4.1.1** Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 4 are managed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Expectations, controls, and oversight for meeting activities within Requirement 4 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.		

Exhibit 22A-4

<table>
<tr><th colspan="2">Requirements and Testing Procedures</th><th>Guidance</th></tr>
<tr><th>Defined Approach Requirements</th><th>Defined Approach Testing Procedures</th><td rowspan="5"><b>Purpose</b>
If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and critical activities may not occur.
<b>Good Practice</b>
Roles and responsibilities may be documented within policies and procedures or maintained within separate documents.
As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities.
<b>Examples</b>
A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).</td></tr>
<tr><td rowspan="2"><b>4.1.2</b> Roles and responsibilities for performing activities in Requirement 4 are documented, assigned, and understood.</td><td><b>4.1.2.a</b> Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 4 are documented and assigned.</td></tr>
<tr><td rowspan="3"><b>4.1.2.b</b> Interview personnel with responsibility for performing activities in Requirement 4 to verify that roles and responsibilities are assigned as documented and are understood.</td></tr>
<tr><th>Customized Approach Objective</th></tr>
<tr><td>Day-to-day responsibilities for performing all the activities in Requirement 4 are allocated. Personnel are accountable for successful, continuous operation of these requirements.</td><td></td></tr>
</table>

Exhibit 22A-4

Requirements and Testing Procedures		Guidance
4.2 PAN is protected with strong cryptography during transmission.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Sensitive information must be encrypted during transmission over public networks because it is easy and common for a malicious individual to intercept and/or divert data while in transit. **Good Practice** The network and data-flow diagrams defined in Requirement 1 are useful resources for identifying all connection points where account data is transmitted or received over open, public networks. While not required, it is considered a good practice for entities to also encrypt PAN over their internal networks, and for entities to establish any new network implementations with encrypted communications. PAN transmissions can be protected by encrypting the data before it is transmitted, or by encrypting the session over which the data is transmitted, or both. While it is not required that strong cryptography be applied at both the data level and the session level, it is strongly recommended. If encrypted at the data level, the cryptographic keys used for protecting the data can be managed in accordance with Requirements 3.6 and 3.7. If the data is encrypted at the session level, designated key custodians should be assigned responsibility for managing transmission keys and certificates. *(continued on next page)*
4.2.1 Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmission over open, public networks: • Only trusted keys and certificates are accepted. • Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked. *This bullet is a best practice until its effective date; refer to applicability notes below for details.* • The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations. • The encryption strength is appropriate for the encryption methodology in use.	**4.2.1.a** Examine documented policies and procedures and interview personnel to verify processes are defined to include all elements specified in this requirement. **4.2.1.b** Examine system configurations to verify that strong cryptography and security protocols are implemented in accordance with all elements specified in this requirement. **4.2.1.c** Examine cardholder data transmissions to verify that all PAN is encrypted with strong cryptography when it is transmitted over open, public networks. **4.2.1.d** Examine system configurations to verify that keys and/or certificates that cannot be verified as trusted are rejected.	
Customized Approach Objective		
Cleartext PAN cannot be read or intercepted from any transmissions over open, public networks.		

Exhibit 22A-4

Requirements and Testing Procedures		Guidance
Applicability Notes A self-signed certificate may also be acceptable if the certificate is issued by an internal CA within the organization, the certificate's author is confirmed, and the certificate is verified—for example, via hash or signature—and has not expired. *The bullet above (for confirming that certificates used to safeguard PAN during transmission over open, public networks are valid and are not expired or revoked) is a best practice until 31 March 2025, after which it will be required as part of Requirement 4.2.1 and must be fully considered during a PCI DSS assessment.*		Some protocol implementations (such as SSL, SSH v1.0, and early TLS) have known vulnerabilities that an attacker can use to gain access to the cleartext data. It is critical that entities maintain awareness of industry-defined deprecation dates for the cipher suites they are using and are prepared to migrate to newer versions or protocols when older ones are no longer deemed secure. Verifying that certificates are trusted helps ensure the integrity of the secure connection. To be considered trusted, a certificate should be issued from a trusted source, such as a trusted certificate authority (CA), and not be expired. Up-to-date Certificate Revocation Lists (CRLs) or Online Certificate Status Protocol (OCSP) can be used to validate certificates. Techniques to validate certificates may include certificate and public key pinning, where the trusted certificate or a public key is pinned either during development or upon its first use. Entities can also confirm with developers or review source code to ensure that clients and servers reject connections if the certificate is bad. For browser-based TLS certificates, certificate trust can often be verified by clicking on the lock icon that appears next to the address bar. *(continued on next page)*

Exhibit 22A-4

Requirements and Testing Procedures		Guidance
4.2.1 *(continued)*		**Examples** Open, public networks include, but are not limited to: • The Internet and • Wireless technologies, including Wi-Fi, Bluetooth, cellular technologies, and satellite communications. **Further Information** Vendor recommendations and industry best practices can be consulted for information about the proper encryption strength specific to the encryption methodology in use. For more information about strong cryptography and secure protocols, see industry standards and best practices such as *NIST SP 800-52* and *SP 800-57*. For more information about trusted keys and certificates, see *NIST Cybersecurity Practice Guide Special Publication 1800-16*, *Securing Web Transactions: Transport Layer Security (TLS) Server Certificate Management.*

Exhibit 22A-4

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** The inventory of trusted keys helps the entity keep track of the algorithms, protocols, key strength, key custodians, and key expiry dates. This enables the entity to respond quickly to vulnerabilities discovered in encryption software, certificates, and cryptographic algorithms. **Good Practice** For certificates, the inventory should include the issuing CA and certification expiration date.
4.2.1.1 An inventory of the entity's trusted keys and certificates used to protect PAN during transmission is maintained.	**4.2.1.1.a** Examine documented policies and procedures to verify processes are defined for the entity to maintain an inventory of its trusted keys and certificates.	
	4.2.1.1.b Examine the inventory of trusted keys and certificates to verify it is kept up to date.	
Customized Approach Objective		
All keys and certificates used to protect PAN during transmission are identified and confirmed as trusted.		
Applicability Notes		
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.		

Exhibit 22A-4

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Since wireless networks do not require physical media to connect, it is important to establish controls limiting who can connect and what transmission protocols will be used. Malicious users use free and widely available tools to eavesdrop on wireless communications. Use of strong cryptography can help limit disclosure of sensitive information across wireless networks. Wireless networks present unique risks to an organization; therefore, they must be identified and protected according to industry requirements. Strong cryptography for authentication and transmission of PAN is required to prevent malicious users from gaining access to the wireless network or utilizing wireless networks to access other internal networks or data. **Good Practice** Wireless networks should not permit fallback or downgrade to an insecure protocol or lower encryption strength that does not meet the intent of strong cryptography. **Further Information** Review the vendor’s specific documentation for more details on the choice of protocols, configurations, and settings related to cryptography.
4.2.1.2 Wireless networks transmitting PAN or connected to the CDE use industry best practices to implement strong cryptography for authentication and transmission.	**4.2.1.2** Examine system configurations to verify that wireless networks transmitting PAN or connected to the CDE use industry best practices to implement strong cryptography for authentication and transmission.	
Customized Approach Objective		
Cleartext PAN cannot be read or intercepted from wireless network transmissions.		

Exhibit 22A-4

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** End-user messaging technologies typically can be easily intercepted by packet-sniffing during delivery across internal and public networks. **Good Practice** The use of end-user messaging technology to send PAN should only be considered where there is a defined business need and should be controlled through the Acceptable Use Policies for end-user technologies defined by the entity according to Requirement 12.2.1. **Examples** E-mail, instant messaging, SMS, and chat are examples of the type of end-user messaging technology that this requirement refers to.
4.2.2 PAN is secured with strong cryptography whenever it is sent via end-user messaging technologies.	**4.2.2.a** Examine documented policies and procedures to verify that processes are defined to secure PAN with strong cryptography whenever sent over end-user messaging technologies.	
	4.2.2.b Examine system configurations and vendor documentation to verify that PAN is secured with strong cryptography whenever it is sent via end-user messaging technologies.	
Customized Approach Objective		
Cleartext PAN cannot be read or intercepted from transmissions using end-user messaging technologies.		
Applicability Notes		
This requirement also applies if a customer, or other third party, requests that PAN is sent to them via end-user messaging technologies. There could be occurrences where an entity receives unsolicited cardholder data via an insecure communication channel that was not intended for transmissions of sensitive data. In this situation, the entity can choose to either include the channel in the scope of their CDE and secure it according to PCI DSS or delete the cardholder data and implement measures to prevent the channel from being used for cardholder data.		

Exhibit 22A-5

Maintain a Vulnerability Management Program

Requirement 5: Protect All Systems and Networks from Malicious Software

Sections

5.1 Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.

5.2 Malicious software (malware) is prevented, or detected and addressed.

5.3 Anti-malware mechanisms and processes are active, maintained, and monitored.

5.4 Anti-phishing mechanisms protect users against phishing attacks.

Overview

Malicious software (malware) is software or firmware designed to infiltrate or damage a computer system without the owner's knowledge or consent, with the intent of compromising the confidentiality, integrity, or availability of the owner’s data, applications, or operating system.

Examples include viruses, worms, Trojans, spyware, ransomware, keyloggers, rootkits, malicious code, scripts, and links.

Malware can enter the network during many business-approved activities, including employee e-mail (for example, via phishing) and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities.

Using anti-malware solutions that address all types of malware helps to protect systems from current and evolving malware threats.

Refer to *Appendix G* for definitions of PCI DSS terms.

Exhibit 22A-5

Requirements and Testing Procedures		Guidance
5.1 Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Requirement 5.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 5. While it is important to define the specific policies or procedures called out in Requirement 5, it is equally important to ensure they are properly documented, maintained, and disseminated. **Good Practice** It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle. **Definitions** Security policies define the entity's security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives.
5.1.1 All security policies and operational procedures that are identified in Requirement 5 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	**5.1.1** Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 5 are managed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Expectations, controls, and oversight for meeting activities within Requirement 5 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.		

Exhibit 22A-5

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If roles and responsibilities are not formally assigned, networks and systems may not be properly protected from malware. **Good Practice** Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities. **Examples** A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).
5.1.2 Roles and responsibilities for performing activities in Requirement 5 are documented, assigned, and understood.	**5.1.2.a** Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 5 are documented and assigned.	
	5.1.2.b Interview personnel with responsibility for performing activities in Requirement 5 to verify that roles and responsibilities are assigned as documented and are understood.	
Customized Approach Objective		
Day-to-day responsibilities for performing all the activities in Requirement 5 are allocated. Personnel are accountable for successful, continuous operation of these requirements.		

Exhibit 22A-5

Requirements and Testing Procedures		Guidance
5.2 Malicious software (malware) is prevented, or detected and addressed.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** There is a constant stream of attacks targeting newly discovered vulnerabilities in systems previously regarded as secure. Without an anti-malware solution that is updated regularly, new forms of malware can be used to attack systems, disable a network, or compromise data. **Good Practice** It is beneficial for entities to be aware of "zero-day" attacks (those that exploit a previously unknown vulnerability) and consider solutions that focus on behavioral characteristics and will alert and react to unexpected behavior. **Definitions** System components known to be affected by malware have active malware exploits available in the real world (not only theoretical exploits).
5.2.1 An anti-malware solution(s) is deployed on all system components, except for those system components identified in periodic evaluations per Requirement 5.2.3 that concludes the system components are not at risk from malware.	**5.2.1.a** Examine system components to verify that an anti-malware solution(s) is deployed on all system components, except for those determined to not be at risk from malware based on periodic evaluations per Requirement 5.2.3.	
Customized Approach Objective	**5.2.1.b** For any system components without an anti-malware solution, examine the periodic evaluations to verify the component was evaluated and the evaluation concludes that the component is not at risk from malware.	
Automated mechanisms are implemented to prevent systems from becoming an attack vector for malware.		

Exhibit 22A-5

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** It is important to protect against all types and forms of malware to prevent unauthorized access. **Good Practice** Anti-malware solutions may include a combination of network-based controls, host-based controls, and endpoint security solutions. In addition to signature-based tools, capabilities used by modern anti-malware solutions include sandboxing, privilege escalation controls, and machine learning. Solution techniques include preventing malware from getting into the network and removing or containing malware that does get into the network. **Examples** Types of malware include, but are not limited to, viruses, Trojans, worms, spyware, ransomware, keyloggers, rootkits, malicious code, scripts, and links.
5.2.2 The deployed anti-malware solution(s): • Detects all known types of malware. • Removes, blocks, or contains all known types of malware.	**5.2.2** Examine vendor documentation and configurations of the anti-malware solution(s) to verify that the solution: • Detects all known types of malware. • Removes, blocks, or contains all known types of malware.	
Customized Approach Objective		
Malware cannot execute or infect other system components.		

Exhibit 22A-5

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
5.2.3 Any system components that are not at risk for malware are evaluated periodically to include the following: • A documented list of all system components not at risk for malware. • Identification and evaluation of evolving malware threats for those system components. • Confirmation whether such system components continue to not require anti-malware protection.	**5.2.3.a** Examine documented policies and procedures to verify that a process is defined for periodic evaluations of any system components that are not at risk for malware that includes all elements specified in this requirement. **5.2.3.b** Interview personnel to verify that the evaluations include all elements specified in this requirement. **5.2.3.c** Examine the list of system components identified as not at risk of malware and compare to the system components without an anti-malware solution deployed per Requirement 5.2.1 to verify that the system components match for both requirements.	Certain systems, at a given point in time, may not currently be commonly targeted or affected by malware. However, industry trends for malware can change quickly, so it is important for organizations to be aware of new malware that might affect their systems—for example, by monitoring vendor security notices and anti-malware forums to determine whether its systems might be coming under threat from new and evolving malware. **Good Practice** If an entity determines that a particular system is not susceptible to any malware, the determination should be supported by industry evidence, vendor resources, and best practices. The following steps can help entities during their periodic evaluations: • Identification of all system types previously determined to not require malware protection. • Review of industry vulnerability alerts and notices to determine if new threats exist for any identified system. • A documented conclusion about whether the system types remain not susceptible to malware. • A strategy to add malware protection for any system types for which malware protection has become necessary. Trends in malware should be included in the identification of new security vulnerabilities at Requirement 6.3.1, and methods to address new trends should be incorporated into the entity's configuration standards and protection mechanisms as needed.
Customized Approach Objective		
The entity maintains awareness of evolving malware threats to ensure that any systems not protected from malware are not at risk of infection.		
Applicability Notes		
System components covered by this requirement are those for which there is no anti-malware solution deployed per Requirement 5.2.1.		

Exhibit 22A-5

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Entities determine the optimum period to undertake the evaluation based on criteria such as the complexity of each entity's environment and the number of types of systems that are required to be evaluated.
5.2.3.1 The frequency of periodic evaluations of system components identified as not at risk for malware is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.	**5.2.3.1.a** Examine the entity's targeted risk analysis for the frequency of periodic evaluations of system components identified as not at risk for malware to verify the risk analysis was performed in accordance with all elements specified in Requirement 12.3.1.	
	5.2.3.1.b Examine documented results of periodic evaluations of system components identified as not at risk for malware and interview personnel to verify that evaluations are performed at the frequency defined in the entity's targeted risk analysis performed for this requirement.	
Customized Approach Objective		
Systems not known to be at risk from malware are re-evaluated at a frequency that addresses the entity's risk.		
Applicability Notes		
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.		

Exhibit 22A-5

Requirements and Testing Procedures		Guidance
5.3 Anti-malware mechanisms and processes are active, maintained, and monitored.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** For an anti-malware solution to remain effective, it needs to have the latest security updates, signatures, threat analysis engines, and any other malware protections on which the solution relies. Having an automated update process avoids burdening end users with responsibility for manually installing updates and provides greater assurance that anti-malware protection mechanisms are updated as quickly as possible after an update is released. **Good Practice** Anti-malware mechanisms should be updated via a trusted source as soon as possible after an update is available. Using a trusted common source to distribute updates to end-user systems helps ensure the integrity and consistency of the solution architecture. Updates may be automatically downloaded to a central location—for example, to allow for testing—prior to being deployed to individual system components.
5.3.1 The anti-malware solution(s) is kept current via automatic updates.	**5.3.1.a** Examine anti-malware solution(s) configurations, including any master installation of the software, to verify the solution is configured to perform automatic updates.	
	5.3.1.b Examine system components and logs, to verify that the anti-malware solution(s) and definitions are current and have been promptly deployed	
Customized Approach Objective		
Anti-malware mechanisms can detect and address the latest malware threats.		

Exhibit 22A-5

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Periodic scans can identify malware that is present, but currently inactive, within the environment. Some malware, such as zero-day malware, can enter an environment before the scan solution is capable of detecting it. Performing regular periodic scans or continuous behavioral analysis of systems or processes helps ensure that previously undetectable malware can be identified, removed, and investigated to determine how it gained access to the environment. **Good Practice** Using a combination of periodic scans (scheduled and on-demand) and active, real-time (on-access) scanning helps ensure that malware residing in both static and dynamic elements of the CDE is addressed. Users should also be able to run on-demand scans on their systems if suspicious activity is detected – this can be useful in the early detection of malware. Scans should include the entire file system, including all disks, memory, and start-up files and boot records (at system restart) to detect all malware upon file execution, including any software that may be resident on a system but not currently active. Scan scope should include all systems and software in the CDE, including those that are often overlooked such as email servers, web browsers, and instant messaging software. **Definitions** Active, or real-time, scanning checks files for malware upon any attempt to open, close, rename, or otherwise interact with a file, preventing the malware from being activated.
5.3.2 The anti-malware solution(s): • Performs periodic scans and active or real-time scans. **OR** • Performs continuous behavioral analysis of systems or processes.	**5.3.2.a** Examine anti-malware solution(s) configurations, including any master installation of the software, to verify the solution(s) is configured to perform at least one of the elements specified in this requirement.	
	5.3.2.b Examine system components, including all operating system types identified as at risk for malware, to verify the solution(s) is enabled in accordance with at least one of the elements specified in this requirement.	
Customized Approach Objective	**5.3.2.c** Examine logs and scan results to verify that the solution(s) is enabled in accordance with at least one of the elements specified in this requirement.	
Malware cannot complete execution.		

Exhibit 22A-5

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Entities can determine the optimum period to undertake periodic scans based on their own assessment of the risks posed to their environments.
5.3.2.1 If periodic malware scans are performed to meet Requirement 5.3.2, the frequency of scans is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.	**5.3.2.1.a** Examine the entity's targeted risk analysis for the frequency of periodic malware scans to verify the risk analysis was performed in accordance with all elements specified in Requirement 12.3.1.	
	5.3.2.1.b Examine documented results of periodic malware scans and interview personnel to verify scans are performed at the frequency defined in the entity's targeted risk analysis performed for this requirement.	
Customized Approach Objective		
Scans by the malware solution are performed at a frequency that addresses the entity's risk.		
Applicability Notes		
This requirement applies to entities conducting periodic malware scans to meet Requirement 5.3.2. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

Exhibit 22A-5

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Portable media devices are often overlooked as an entry method for malware. Attackers will often pre-load malware onto portable devices such as USB and flash drives; connecting an infected device to a computer then triggers the malware, introducing new threats within the environment.
5.3.3 For removable electronic media, the anti-malware solution(s): • Performs automatic scans of when the media is inserted, connected, or logically mounted, **OR** • Performs continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted.	**5.3.3.a** Examine anti-malware solution(**s)** configurations to verify that, for removable electronic media, the solution is configured to perform at least one of the elements specified in this requirement.	
	5.3.3.b Examine system components with removable electronic media connected to verify that the solution(s) is enabled in accordance with at least one of the elements as specified in this requirement.	
Customized Approach Objective	**5.3.3.c** Examine logs and scan results to verify that the solution(s) is enabled in accordance with at least one of the elements specified in this requirement.	
Malware cannot be introduced to system components via external removable media.		
Applicability Notes		
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.		

Exhibit 22A-5

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** It is important to track the effectiveness of the anti-malware mechanisms—for example, by confirming that updates and scans are being performed as expected, and that malware is identified and addressed. Audit logs also allow an entity to determine how malware entered the environment and track its activity when inside the entity's network.
5.3.4 Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1.	**5.3.4** Examine anti-malware solution(s) configurations to verify logs are enabled and retained in accordance with Requirement 10.5.1.	
Customized Approach Objective		
Historical records of anti-malware actions are immediately available and retained for at least 12 months.		

Exhibit 22A-5

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** It is important that defensive mechanisms are always running so that malware is detected in real time. Ad-hoc starting and stopping of anti-malware solutions could allow malware to propagate unchecked and undetected. **Good Practice** Where there is a legitimate need to temporarily disable a system's anti-malware protection—for example, to support a specific maintenance activity or investigation of a technical problem—the reason for taking such action should be understood and approved by an appropriate management representative. Any disabling or altering of anti-malware mechanisms, including on administrators' own devices, should be performed by authorized personnel. It is recognized that administrators have privileges that may allow them to disable anti-malware on their own computers, but there should be alerting mechanisms in place when such software is disabled and then follow up that occurs to ensure correct processes were followed. **Examples** Additional security measures that may need to be implemented for the period during which anti-malware protection is not active include disconnecting the unprotected system from the Internet while the anti-malware protection is disabled and running a full scan once it is re-enabled.
5.3.5 Anti-malware mechanisms cannot be disabled or altered by users, unless specifically documented, and authorized by management on a case-by-case basis for a limited time period.	**5.3.5.a** Examine anti-malware configurations, to verify that the anti-malware mechanisms cannot be disabled or altered by users.	
Customized Approach Objective	**5.3.5.b** Interview responsible personnel and observe processes to verify that any requests to disable or alter anti-malware mechanisms are specifically documented and authorized by management on a case-by-case basis for a limited time period.	
Anti-malware mechanisms cannot be modified by unauthorized personnel.		
Applicability Notes		
Anti-malware solutions may be temporarily disabled only if there is a legitimate technical need, as authorized by management on a case-by-case basis. If anti-malware protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period during which anti-malware protection is not active.		

Exhibit 22A-5

Requirements and Testing Procedures		Guidance
5.4 Anti-phishing mechanisms protect users against phishing attacks.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Technical controls can limit the number of occasions personnel have to evaluate the veracity of a communication and can also limit the effects of individual responses to phishing. **Good Practice** When developing anti-phishing controls, entities are encouraged to consider a combination of approaches. For example, using anti-spoofing controls such as Domain-based Message Authentication, Reporting & Conformance (DMARC), Sender Policy Framework (SPF), and Domain Keys Identified Mail (DKIM) will help stop phishers from spoofing the entity's domain and impersonating personnel. The deployment of technologies for blocking phishing emails and malware before they reach personnel, such as link scrubbers and server-side anti-malware, can reduce incidents and decrease the time required by personnel to check and report phishing attacks. Additionally, training personnel to recognize and report phishing emails can allow similar emails to be identified and permit them to be removed before being opened. It is recommended (but not required) that anti-phishing controls are applied across an entity's entire organization. *(continued on next page)*
5.4.1 Processes and automated mechanisms are in place to detect and protect personnel against phishing attacks.	**5.4.1** Observe implemented processes and examine mechanisms to verify controls are in place to detect and protect personnel against phishing attacks.	
Customized Approach Objective		
Mechanisms are in place to protect against and mitigate risk posed by phishing attacks.		
Applicability Notes		
The focus of this requirement is on protecting personnel with access to system components in-scope for PCI DSS. Meeting this requirement for technical and automated controls to detect and protect personnel against phishing is not the same as Requirement 12.6.3.1 for security awareness training. Meeting this requirement does not also meet the requirement for providing personnel with security awareness training, and vice versa. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

Exhibit 22A-5

Requirements and Testing Procedures		Guidance
5.4.1 *(continued)*		**Definitions** Phishing is a form of social engineering and describes the different methods used by attackers to trick personnel into disclosing sensitive information, such as user account names and passwords, and account data. Attackers will typically disguise themselves and attempt to appear as a genuine or trusted source, directing personnel to send an email response, click on a web link, or enter data into a compromised website. Mechanisms that can detect and prevent phishing attempts are often included in anti-malware solutions. **Further Information** See the following for more information about phishing: *National Cyber Security Centre - Phishing Attacks: Defending your Organization*. *US Cybersecurity & Infrastructure Security Agency - Report Phishing Sites.*

Exhibit 22A-6

Requirement 6: Develop and Maintain Secure Systems and Software

Sections

6.1 Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.

6.2 Bespoke and custom software are developed securely.

6.3 Security vulnerabilities are identified and addressed.

6.4 Public-facing web applications are protected against attacks.

6.5 Changes to all system components are managed securely.

Overview

Actors with bad intentions can use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor provided security patches, which must be installed by the entities that manage the systems. All system components must have all appropriate software patches to protect against the exploitation and compromise of account data by malicious individuals and malicious software.

Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For bespoke and custom software, numerous vulnerabilities can be avoided by applying software lifecycle (SLC) processes and secure coding techniques.

Code repositories that store application code, system configurations, or other configuration data that can impact the security of cardholder data and/or sensitive authentication data are in scope for PCI DSS assessments.

See *Relationship between PCI DSS and PCI SSC Software Standards* on page 7 for information about the use of PCI SSC-validated software and software vendors, and how use of PCI SSC's software standards may help with meeting controls in Requirement 6.

Refer to *Appendix G* for definitions of PCI DSS terms.

***Note**: Requirement 6 applies to all system components, except for section 6.2 for developing software securely, which applies only to bespoke and custom software used on any system component included in or connected to the CDE.*

Exhibit 22A-6

Requirements and Testing Procedures		Guidance
6.1 Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Requirement 6.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 6. While it is important to define the specific policies or procedures called out in Requirement 6, it is equally important to ensure they are properly documented, maintained, and disseminated. **Good Practice** It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle. **Definitions** Security policies define the entity's security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives.
6.1.1 All security policies and operational procedures that are identified in Requirement 6 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	**6.1.1** Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 6 are managed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Expectations, controls, and oversight for meeting activities within Requirement 6 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.		

Exhibit 22A-6

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If roles and responsibilities are not formally assigned, systems will not be securely maintained, and their security level will be reduced. **Good Practice** Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities. **Examples** A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).
6.1.2 Roles and responsibilities for performing activities in Requirement 6 are documented, assigned, and understood.	**6.1.2.a** Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 6 are documented and assigned.	
Customized Approach Objective	**6.1.2.b** Interview personnel responsible for performing activities in Requirement 6 to verify that roles and responsibilities are assigned as documented and are understood.	
Day-to-day responsibilities for performing all the activities in Requirement 6 are allocated. Personnel are accountable for successful, continuous operation of these requirements.		

Exhibit 22A-6

Requirements and Testing Procedures		Guidance
6.2 Bespoke and custom software are developed securely.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Without the inclusion of security during the requirements definition, design, analysis, and testing phases of software development, security vulnerabilities can be inadvertently or maliciously introduced into the production environment. **Good Practice** Understanding how sensitive data is handled by the application—including when stored, transmitted, and in memory—can help identify where data needs to be protected. PCI DSS requirements must be considered when developing software to meet those requirements by design, rather than trying to retrofit the software later. **Examples** Secure software lifecycle management methodologies and frameworks include PCI Software Security Framework, BSIMM, OPENSAMM, and works from NIST, ISO, and SAFECode.
6.2.1 Bespoke and custom software are developed securely, as follows: • Based on industry standards and/or best practices for secure development. • In accordance with PCI DSS (for example, secure authentication and logging). • Incorporating consideration of information security issues during each stage of the software development lifecycle.	**6.2.1** Examine documented software development procedures to verify that processes are defined that include all elements specified in this requirement.	
Customized Approach Objective		
Bespoke and custom software is developed in accordance with PCI DSS and secure development processes throughout the software lifecycle.		
Applicability Notes		
This applies to all software developed for or by the entity for the entity's own use. This includes both bespoke and custom software. This does not apply to third-party software.		

Exhibit 22A-6

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Having staff knowledgeable in secure coding methods, including techniques defined in Requirement 6.2.4, will help minimize the number of security vulnerabilities introduced through poor coding practices. **Good Practice** Training for developers may be provided in-house or by third parties. Training should include, but is not limited to, development languages in use, secure software design, secure coding techniques, use of techniques/methods for finding vulnerabilities in code, processes to prevent reintroducing previously resolved vulnerabilities, and how to use any automated security testing tools for detecting vulnerabilities in software. As industry-accepted secure coding practices change, organizational coding practices and developer training may need to be updated to address new threats.
6.2.2 Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows: • On software security relevant to their job function and development languages. • Including secure software design and secure coding techniques. • Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.	**6.2.2.a** Examine software development procedures to verify that processes are defined for training of software development personnel developing bespoke and custom software that includes all elements specified in this requirement.	
	6.2.2.b Examine training records and interview personnel to verify that software development personnel working on bespoke and custom software received software security training that is relevant to their job function and development languages in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Software development personnel remain knowledgeable about secure development practices; software security; and attacks against the languages, frameworks, or applications they develop. Personnel are able to access assistance and guidance when required.		

Exhibit 22A-6

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Security vulnerabilities in bespoke and custom software are commonly exploited by malicious individuals to gain access to a network and compromise account data. Vulnerable code is far more difficult and expensive to address after it has been deployed or released into production environments. Requiring a formal review and signoff by management prior to release helps to ensure that code is approved and has been developed in accordance with policies and procedures. **Good Practice** The following items should be considered for inclusion in code reviews: • Searching for undocumented features (implant tools, backdoors). • Confirming that software securely uses external components' functions (libraries, frameworks, APIs, etc.). For example, if a third-party library providing cryptographic functions is used, verify that it was integrated securely. • Checking for correct use of logging to prevent sensitive data from getting into logs. • Analysis of insecure code structures that may contain potential vulnerabilities related to common software attacks identified in Requirement 6.2.4. • Checking the application's behavior to detect logical vulnerabilities.
6.2.3 Bespoke and custom software is reviewed prior to being released into production or to customers, to identify and correct potential coding vulnerabilities, as follows: • Code reviews ensure code is developed according to secure coding guidelines. • Code reviews look for both existing and emerging software vulnerabilities. • Appropriate corrections are implemented prior to release.	**6.2.3.a** Examine documented software development procedures and interview responsible personnel to verify that processes are defined that require all bespoke and custom software to be reviewed in accordance with all elements specified in this requirement. **6.2.3.b** Examine evidence of changes to bespoke and custom software to verify that the code changes were reviewed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Bespoke and custom software cannot be exploited via coding vulnerabilities.		
Applicability Notes		
This requirement for code reviews applies to all bespoke and custom software (both internal and public facing), as part of the system development lifecycle. Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.4. Code reviews may be performed using either manual or automated processes, or a combination of both.		

Exhibit 22A-6

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Having code reviewed by someone other than the original author, who is both experienced in code reviews and knowledgeable about secure coding practices, minimizes the possibility that code containing security or logic errors that could affect the security of cardholder data is released into a production environment. Requiring management approval that the code was reviewed limits the ability for the process to be bypassed. **Good Practice** Having a formal review methodology and review checklists has been found to improve the quality of the code review process. Code review is a tiring process, and for this reason, it is most effective when reviewers only review small amounts of code at a time. To maintain the effectiveness of code reviews, it is beneficial to monitor the general workload of reviewers and to have them review applications they are familiar with. Code reviews may be performed using either manual or automated processes, or a combination of both. Entitles that rely solely on manual code review should ensure that reviewers maintain their skills through regular training as new vulnerabilities are found, and new secure coding methods are recommended. **Further Information** See the *OWASP Code Review Guide*.
6.2.3.1 If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are: • Reviewed by individuals other than the originating code author, and who are knowledgeable about code-review techniques and secure coding practices. • Reviewed and approved by management prior to release.	**6.2.3.1.a** If manual code reviews are performed for bespoke and custom software prior to release to production, examine documented software development procedures and interview responsible personnel to verify that processes are defined for manual code reviews to be conducted in accordance with all elements specified in this requirement. **6.2.3.1.b** Examine evidence of changes to bespoke and custom software and interview personnel to verify that manual code reviews were conducted in accordance with all elements specified in this requirement.	
Customized Approach Objective		
The manual code review process cannot be bypassed and is effective at discovering security vulnerabilities.		
Applicability Notes		
Manual code reviews can be conducted by knowledgeable internal personnel or knowledgeable third-party personnel. An individual that has been formally granted accountability for release control and who is neither the original code author nor the code reviewer fulfills the criteria of being management.		

Exhibit 22A-6

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Detecting or preventing common errors that result in vulnerable code as early as possible in the software development process lowers the probability that such errors make it through to production and lead to a compromise. Having formal engineering techniques and tools embedded in the development process will catch these errors early. This philosophy is sometimes called "shifting security left." **Good Practice** For both bespoke and custom software, the entity must ensure that code is developed focusing on the prevention or mitigation of common software attacks, including: • Attempts to exploit common coding vulnerabilities (bugs). • Attempts to exploit software design flaws. • Attempts to exploit implementation/configuration flaws. • Enumeration attacks – automated attacks that are actively exploited in payments and abuse identification, authentication, or authorization mechanisms. See the *PCI Perspectives blog article "Beware of Account Testing Attacks*." *(continued on next page)*
6.2.4 Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following: • Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws. • Attacks on data and data structures, including attempts to manipulate buffers, pointers, input data, or shared data. • Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation. • Attacks on business logic, including attempts to abuse or bypass application features and functionalities through the manipulation of APIs, communication protocols and channels, client-side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF). • Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms. • Attacks via any "high-risk" vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1.	**6.2.4** Examine documented procedures and interview responsible software development personnel to verify that software engineering techniques or other methods are defined and in use by developers of bespoke and custom software to prevent or mitigate all common software attacks as specified in this requirement.	

Exhibit 22A-6

Requirements and Testing Procedures		Guidance
Customized Approach Objective Bespoke and custom software cannot be exploited via common attacks and related vulnerabilities. **Applicability Notes** This applies to all software developed for or by the entity for the entity's own use. This includes both bespoke and custom software. This does not apply to third-party software.		Researching and documenting software engineering techniques or other methods helps to define how software developers prevent or mitigate various software attacks by features or countermeasures they build into software. This might include identification/authentication mechanisms, access control, input validation routines, etc. Developers should be familiar with different types of vulnerabilities and potential attacks and use measures to avoid potential attack vectors when developing code. **Examples** Techniques include automated processes and practices that scan code early in the development cycle when code is checked in to confirm the vulnerabilities are not present.

Exhibit 22A-6

Requirements and Testing Procedures		Guidance
6.3 Security vulnerabilities are identified and addressed.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Classifying the risks (for example, as critical, high, medium, or low) allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited. **Good Practice** Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy. When an entity is assigning its risk rankings, it should consider using a formal, objective, justifiable methodology that accurately portrays the risks of the vulnerabilities pertinent to the organization and translates to an appropriate entity-assigned priority for resolution. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data. *(continued on next page)*
6.3.1 Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). • Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. • Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. • Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	**6.3.1.a** Examine policies and procedures for identifying and managing security vulnerabilities to verify that processes are defined in accordance with all elements specified in this requirement. **6.3.1.b** Interview responsible personnel, examine documentation, and observe processes to verify that security vulnerabilities are identified and managed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
New system and software vulnerabilities that may impact the security of cardholder data and/or sensitive authentication data are monitored, cataloged, and risk assessed.		

Exhibit 22A-6

Requirements and Testing Procedures		Guidance
Applicability Notes This requirement is not achieved by, and is in addition to, performing vulnerability scans according to Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability.		An organization's processes for managing vulnerabilities should be integrated with other management processes—for example, risk management, change management, patch management, incident response, application security, as well as proper monitoring and logging of these processes. This process should include multiple sources of vulnerability information, including industry-recognized vulnerability databases (for example, the US National Vulnerability Database), CERTs, RSS feeds, information received from vendors and third parties, and vulnerabilities identified via internal and external vulnerability scans (Requirements 11.3.1 and 11.3.2). This will help to ensure all vulnerabilities are properly identified and addressed. Processes should support ongoing evaluation of vulnerabilities. For example, a vulnerability initially identified as low risk could become a higher risk later. Additionally, vulnerabilities individually considered to be low or medium risk, could collectively pose a high or critical risk if present on the same system, or if exploited on a low-risk system that could result in access to the CDE. *(continued on next page)*

Exhibit 22A-6

Requirements and Testing Procedures		Guidance
6.3.1 *(continued)*		**Examples** Some organizations that issue alerts to advise entities about urgent vulnerabilities requiring immediate patches/updates are national Computer Emergency Readiness/Response Teams (CERTs) and vendors. Criteria for ranking vulnerabilities may include criticality of a vulnerability identified in an alert from Forum of Incident Response and Security Teams (FIRST) or a CERT, consideration of the CVSS score, the classification by the vendor, and/or type of systems affected. **Further Information** Trustworthy sources for vulnerability information include vendor websites, industry newsgroups, mailing lists, etc. If software is developed in-house, the internal development team should also consider sources of information about new vulnerabilities that may affect internally developed applications. Other methods to ensure new vulnerabilities are identified include solutions that automatically recognize and alert upon detection of unusual behavior. Processes should account for widely published exploits as well as “zero-day” attacks, which target previously unknown vulnerabilities. For bespoke and custom software, the organization may obtain information about libraries, frameworks, compilers, programming languages, etc. from public trusted sources (for example, special resources and resources from component developers). The organization may also independently analyze third-party components and identify vulnerabilities. *(continued on next page)*

Exhibit 22A-6

Requirements and Testing Procedures		Guidance
6.3.1 *(continued)*		For control over in-house developed software, the organization may receive such information from external sources. The organization can consider using a “bug bounty” program where it posts information (for example, on its website) so third parties can contact the organization with vulnerability information. External sources may include independent investigators or companies that report to the organization about identified vulnerabilities and may include sources such as the Common Vulnerability Scoring System (CVSS) or the OWASP Risk Rating Methodology.

Exhibit 22A-6

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Identifying and listing all the entity's bespoke and custom software, and any third-party software that is incorporated into the entity's bespoke and custom software enables the entity to manage vulnerabilities and patches. Vulnerabilities in third-party components (including libraries, APIs, etc.) embedded in an entity's software also renders those applications vulnerable to attacks. Knowing which third-party components are used in the entity's software and monitoring the availability of security patches to address known vulnerabilities is critical to ensuring the security of the software. **Good Practice** An entity's inventory should cover all payment software components and dependencies, including supported execution platforms or environments, third-party libraries, services, and other required functionalities. There are many different types of solutions that can help with managing software inventories, such as software composition analysis tools, application discovery tools, and mobile device management.
6.3.2 An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management.	**6.3.2.a** Examine documentation and interview personnel to verify that an inventory of bespoke and custom software and third-party software components incorporated into bespoke and custom software is maintained, and that the inventory is used to identify and address vulnerabilities.	
Customized Approach Objective		
Known vulnerabilities in third-party software components cannot be exploited in bespoke and custom software.	**6.3.2.b** Examine software documentation, including for bespoke and custom software that integrates third-party software components, and compare it to the inventory to verify that the inventory includes the bespoke and custom software and third-party software components.	
Applicability Notes		
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.		

Exhibit 22A-6

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** New exploits are constantly being discovered, and these can permit attacks against systems that have previously been considered secure. If the most recent security patches/updates are not implemented on critical systems as soon as possible, a malicious actor can use these exploits to attack or disable a system or gain access to sensitive data. **Good Practice** Prioritizing security patches/updates for critical infrastructure ensures that high-priority systems and devices are protected from vulnerabilities as soon as possible after a patch is released. An entity's patching cadence should factor in any re-evaluation of vulnerabilities and subsequent changes in the criticality of a vulnerability per Requirement 6.3.1. For example, a vulnerability initially identified as low risk could become a higher risk later. Additionally, vulnerabilities individually considered to be low or medium risk could collectively pose a high or critical risk if present on the same system, or if exploited on a low-risk system that could result in access to the CDE. *(continued on next page)*
6.3.3 All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: • Patches/updates for critical vulnerabilities (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release. • All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity's assessment of the criticality of the risk to the environment as identified according to the risk ranking process at Requirement 6.3.1.	**6.3.3.a** Examine policies and procedures to verify processes are defined for addressing vulnerabilities by installing applicable security patches/updates in accordance with all elements specified in this requirement.	
	6.3.3.b Examine system components and related software and compare the list of installed security patches/updates to the most recent security patch/update information to verify vulnerabilities are addressed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
System components cannot be compromised via the exploitation of a known vulnerability.		

Exhibit 22A-6

Requirements and Testing Procedures		Guidance
6.3.3 *(continued)*		It is recommended that the entity complete a targeted risk analysis (TRA) according to PCI DSS Requirement 12.3.1 to document the frequency of installing all other applicable security patches/updates. This TRA would include consideration of the entity's assessment of the criticality of the risk to their environment as identified in the risk ranking process at Requirement 6.3.1. **Examples** An example time frame for installation of patches/updates could be 60 days for high-risk vulnerabilities and 90 days for others, as determined by the entity's assessment of risk.

Exhibit 22A-6

Requirements and Testing Procedures		Guidance
6.4 Public-facing web applications are protected against attacks.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Public-facing web applications are those that are available to the public (not only for internal use). These applications are primary targets for attackers, and poorly coded web applications provide an easy path for attackers to gain access to sensitive data and systems. **Good Practice** Manual or automated vulnerability security assessment tools or methods review and/or test the application for vulnerabilities. Common assessment tools include specialized web scanners that perform automatic analysis of web application protection. When using automated technical solutions, it is important to include processes that facilitate timely responses to alerts generated by the solutions so that any detected attacks can be mitigated. **Examples** A web application firewall (WAF) installed in front of public-facing web applications to check all traffic is an example of an automated technical solution that detects and prevents web-based attacks (for example, the attacks included in Requirement 6.2.4). WAFs filter and block non-essential traffic at the application layer. A properly configured WAF helps to prevent application-layer attacks on applications that are improperly coded or configured. *(continued on next page)*
6.4.1 For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows: – At least once every 12 months and after significant changes. – By an entity that specializes in application security. – Including, at a minimum, all common software attacks in Requirement 6.2.4. – All vulnerabilities are ranked in accordance with requirement 6.3.1. – All vulnerabilities are corrected. – The application is re-evaluated after the corrections. **OR** • Installing an automated technical solution(s) that continually detects and prevents web-based attacks as follows: – Installed in front of public-facing web applications to detect and prevent web-based attacks. – Actively running and up to date as applicable. – Generating audit logs. – Configured to either block web-based attacks or generate an alert that is immediately investigated.	**6.4.1** For public-facing web applications, ensure that either one of the required methods is in place as follows: • If manual or automated vulnerability security assessment tools or methods are in use, examine documented processes, interview personnel, and examine records of application security assessments to verify that public-facing web applications are reviewed in accordance with all elements of this requirement specific to the tool/method. **OR** • If an automated technical solution(s) is installed that continually detects and prevents web-based attacks, examine the system configuration settings and audit logs, and interview responsible personnel to verify that the automated technical solution(s) is installed in accordance with all elements of this requirement specific to the solution(s).	

Exhibit 22A-6

Requirements and Testing Procedures		Guidance
Customized Approach Objective Public-facing web applications are protected against malicious attacks. **Applicability Notes** This assessment is not the same as the vulnerability scans performed for Requirement 11.3.1 and 11.3.2. *This requirement will be superseded by Requirement 6.4.2 after 31 March 2025 when Requirement 6.4.2 becomes effective.*		Another example of an automated technical solution is Runtime Application Self-Protection (RASP) technologies. When implemented correctly, RASP solutions can detect and block anomalous behavior by the software during execution. While WAFs typically monitor the application perimeter, RASP solutions monitor and block behavior within the application.

Exhibit 22A-6

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Public-facing web applications are primary targets for attackers, and poorly coded web applications provide an easy path for attackers to gain access to sensitive data and systems. **Good Practice** When using automated technical solutions, it is important to include processes that facilitate timely responses to alerts generated by the solutions so that any detected attacks can be mitigated. Such solutions may also be used to automate mitigation, for example rate-limiting controls, which can be implemented to mitigate against brute-force attacks and enumeration attacks. **Examples** A web application firewall (WAF), which can be either on-premise or cloud-based, installed in front of public-facing web applications to check all traffic, is an example of an automated technical solution that detects and prevents web-based attacks (for example, the attacks included in Requirement 6.2.4). WAFs filter and block non-essential traffic at the application layer. A properly configured WAF helps to prevent application-layer attacks on applications that are improperly coded or configured.
6.4.2 For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following: • Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks. • Actively running and up to date as applicable. • Generating audit logs. • Configured to either block web-based attacks or generate an alert that is immediately investigated.	**6.4.2** For public-facing web applications, examine the system configuration settings and audit logs, and interview responsible personnel to verify that an automated technical solution that detects and prevents web-based attacks is in place in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Public-facing web applications are protected in real time against malicious attacks.		
Applicability Notes		
This new requirement will replace Requirement 6.4.1 once its effective date is reached. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

Exhibit 22A-6

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Scripts loaded and executed in the payment page can have their functionality altered without the entity's knowledge and can also have the functionality to load additional external scripts (for example, advertising and tracking, tag management systems). Such seemingly harmless scripts can be used by potential attackers to upload malicious scripts that can read and exfiltrate cardholder data from the consumer browser. Ensuring that the functionality of all such scripts is understood to be necessary for the operation of the payment page minimizes the number of scripts that could be tampered with. Ensuring that scripts have been explicitly authorized reduces the probability of unnecessary scripts being added to the payment page without appropriate management approval. Where it is impractical for such authorization to occur before a script is changed or a new script is added to the page, the authorization should be confirmed as soon as possible after a change is made. Using techniques to prevent tampering with the script will minimize the probability of the script being modified to carry out unauthorized behavior, such as skimming the cardholder data from the payment page. *(continued on next page)*
6.4.3 All payment page scripts that are loaded and executed in the consumer's browser are managed as follows: • A method is implemented to confirm that each script is authorized. • A method is implemented to assure the integrity of each script. • An inventory of all scripts is maintained with written business or technical justification as to why each is necessary.	**6.4.3.a** Examine policies and procedures to verify that processes are defined for managing all payment page scripts that are loaded and executed in the consumer's browser, in accordance with all elements specified in this requirement. **6.4.3.b** Interview responsible personnel and examine inventory records and system configurations to verify that all payment page scripts that are loaded and executed in the consumer's browser are managed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Unauthorized code cannot be executed in the payment page as it is rendered in the consumer's browser.		

Exhibit 22A-6

Requirements and Testing Procedures		Guidance
Applicability Notes This requirement applies to all scripts loaded from the entity's environment and scripts loaded from third and fourth parties. This requirement also applies to scripts in the entity's webpage(s) that includes a TPSP's/ payment processor's embedded payment page/form (for example, one or more inline frames or iframes). This requirement does not apply to an entity for scripts in a TPSP's/payment processor's embedded payment page/form (for example, one or more iframes), where the entity includes a TPSP's/payment processor's payment page/form on its webpage. Scripts in the TPSP's/payment processor's embedded payment page/form are the responsibility of the TPSP/payment processor to manage in accordance with this requirement. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		**Good Practice** Scripts may be authorized by manual or automated (e.g., workflow) processes. Where the payment page will be loaded into an inline frame (iframe), restricting the location that the payment page can be loaded from, using the parent page's Content Security Policy (CSP) can help prevent unauthorized content being substituted for the payment page. Where an entity includes a TPSP's/payment processor's embedded payment page/form on its webpage, the entity should expect the TPSP/payment processor to provide evidence that the TPSP/payment processor is meeting this requirement, in accordance with the TPSP's/payment processor's PCI DSS assessment and Requirement 12.9. **Examples** The integrity of scripts can be enforced by several different mechanisms including, but not limited to: • Sub-resource integrity (SRI), which allows the consumer browser to validate that a script has not been tampered with. • A CSP, which limits the locations the consumer browser can load a script from and transmit account data to. • Proprietary script or tag-management systems, which can prevent malicious script execution.

Exhibit 22A-6

Requirements and Testing Procedures		Guidance
6.5 Changes to all system components are managed securely.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Change management procedures must be applied to all changes—including the addition, removal, or modification of any system component—in the production environment. It is important to document the reason for a change and the change description so that relevant parties understand and agree the change is needed. Likewise, documenting the impacts of the change allows all affected parties to plan appropriately for any processing changes. **Good Practice** Approval by authorized parties confirms that the change is legitimate and that the change is sanctioned by the organization. Changes should be approved by individuals with the appropriate authority and knowledge to understand the impact of the change. Thorough testing by the entity confirms that the security of the environment is not reduced by implementing a change and that all existing security controls either remain in place or are replaced with equal or stronger security controls after the change. The specific testing to be performed will vary according to the type of change and system component(s) affected. For each change, it is important to have documented procedures that address any failures and provide instructions on how to return to a secure state in case the change fails or adversely affects the security of an application or system. These procedures will allow the application or system to be restored to its previous secure state.
6.5.1 Changes to all system components in the production environment are made according to established procedures that include: - Reason for, and description of, the change. - Documentation of security impact. - Documented change approval by authorized parties. - Testing to verify that the change does not adversely impact system security. - For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production. - Procedures to address failures and return to a secure state.	**6.5.1.a** Examine documented change control procedures to verify procedures are defined for changes to all system components in the production environment to include all elements specified in this requirement.	
	6.5.1.b Examine recent changes to system components and trace those changes back to related change control documentation. For each change examined, verify the change is implemented in accordance with all elements specified in this requirement.	
Customized Approach Objective		
All changes are tracked, authorized, and evaluated for impact and security, and changes are managed to avoid unintended effects to the security of system components.		

Exhibit 22A-6

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Having processes to analyze significant changes helps ensure that all appropriate PCI DSS controls are applied to any systems or networks added or changed within the in-scope environment, and that PCI DSS requirements continue to be met to secure the environment. **Good Practice** Building this validation into change management processes helps ensure that device inventories and configuration standards are kept up to date and security controls are applied where needed. **Examples** Applicable PCI DSS requirements that could be impacted include, but are not limited to: • Network and data-flow diagrams are updated to reflect changes. • Systems are configured per configuration standards, with all default passwords changed and unnecessary services disabled. • Systems are protected with required controls—for example, file integrity monitoring (FIM), anti-malware, patches, and audit logging. • Sensitive authentication data is not stored, and all account data storage is documented and incorporated into data retention policy and procedures. • New systems are included in the quarterly vulnerability scanning process. • Systems are scanned for internal and external vulnerabilities after significant changes per Requirements 11.3.1.3 and 11.3.2.1.
6.5.2 Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.	**6.5.2** Examine documentation for significant changes, interview personnel, and observe the affected systems/networks to verify that the entity confirmed applicable PCI DSS requirements were in place on all new or changed systems and networks and that documentation was updated as applicable.	
Customized Approach Objective		
All system components are verified after a significant change to be compliant with the applicable PCI DSS requirements.		
Applicability Notes		
These significant changes should also be captured and reflected in the entity's annual PCI DSS scope confirmation activity per Requirement 12.5.2.		

Exhibit 22A-6

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Due to the constantly changing state of pre-production environments, they are often less secure than the production environment. **Good Practice** Organizations must clearly understand which environments are test environments or development environments and how these environments interact on the level of networks and applications. **Definitions** Pre-production environments include development, testing, user acceptance testing (UAT), etc. Even where production infrastructure is used to facilitate testing or development, production environments still need to be separated (logically or physically) from pre-production functionality such that vulnerabilities introduced as a result of pre-production activities do not adversely affect production systems.
6.5.3 Pre-production environments are separated from production environments and the separation is enforced with access controls.	**6.5.3.a** Examine policies and procedures to verify that processes are defined for separating the pre-production environment from the production environment via access controls that enforce the separation.	
	6.5.3.b Examine network documentation and configurations of network security controls to verify that the pre-production environment is separate from the production environment(s).	
	6.5.3.c Examine access control settings to verify that access controls are in place to enforce separation between the pre-production and production environment(s).	
Customized Approach Objective		
Pre-production environments cannot introduce risks and vulnerabilities into production environments.		

Exhibit 22A-6

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** The goal of separating roles and functions between production and pre-production environments is to reduce the number of personnel with access to the production environment and account data and thereby minimize risk of unauthorized, unintentional, or inappropriate access to data and system components and help ensure that access is limited to those individuals with a business need for such access. The intent of this control is to separate critical activities to provide oversight and review to catch errors and minimize the chances of fraud or theft (since two people would need to collude in order to hide an activity). Separating roles and functions, also referred to as separation or segregation of duties, is a key internal control concept to protect an entity's assets.
6.5.4 Roles and functions are separated between production and pre-production environments to provide accountability such that only reviewed and approved changes are deployed.	**6.5.4.a** Examine policies and procedures to verify that processes are defined for separating roles and functions to provide accountability such that only reviewed and approved changes are deployed.	
	6.5.4.b Observe processes and interview personnel to verify implemented controls separate roles and functions and provide accountability such that only reviewed and approved changes are deployed.	
Customized Approach Objective		
Job roles and accountability that differentiate between pre-production and production activities are defined and managed to minimize the risk of unauthorized, unintentional, or inappropriate actions.		
Applicability Notes		
In environments with limited personnel where individuals perform multiple roles or functions, this same goal can be achieved with additional procedural controls that provide accountability. For example, a developer may also be an administrator that uses an administrator-level account with elevated privileges in the development environment and, for their developer role, they use a separate account with user-level access to the production environment.		

Exhibit 22A-6

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Use of live PANs outside of protected CDEs provides malicious individuals with the opportunity to gain unauthorized access to cardholder data. **Definitions** Live PANs refer to valid PANs (not test PANs) issued by, or on behalf of, a payment brand. Additionally, when payment cards expire, the same PAN is often reused with a different expiry date. All PANs must be verified as being unable to conduct payment transactions or pose fraud risk to the payment system before they are excluded from PCI DSS scope. It is the responsibility of the entity to confirm that PANs are not live.
6.5.5 Live PANs are not used in pre-production environments, except where those environments are included in the CDE and protected in accordance with all applicable PCI DSS requirements.	**6.5.5.a** Examine policies and procedures to verify that processes are defined for not using live PANs in pre-production environments, except where those environments are in a CDE and protected in accordance with all applicable PCI DSS requirements.	
	6.5.5.b Observe testing processes and interview personnel to verify procedures are in place to ensure live PANs are not used in pre-production environments, except where those environments are in a CDE and protected in accordance with all applicable PCI DSS requirements.	
Customized Approach Objective	**6.5.5.c** Examine pre-production test data to verify live PANs are not used in pre-production environments, except where those environments are in a CDE and protected in accordance with all applicable PCI DSS requirements.	
Live PANs cannot be present in pre-production environments outside the CDE.		

Exhibit 22A-6

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	
6.5.6 Test data and test accounts are removed from system components before the system goes into production.	**6.5.6.a** Examine policies and procedures to verify that processes are defined for removal of test data and test accounts from system components before the system goes into production.	**Purpose** This data may give away information about the functioning of an application or system and is an easy target for unauthorized individuals to exploit to gain access to systems. Possession of such information could facilitate compromise of the system and related account data.
	6.5.6.b Observe testing processes for both off-the-shelf software and in-house applications, and interview personnel to verify test data and test accounts are removed before a system goes into production.	
Customized Approach Objective Test data and test accounts cannot exist in production environments.	**6.5.6.c** Examine data and accounts for recently installed or updated off-the-shelf software and in-house applications to verify there is no test data or test accounts on systems in production.	

Exhibit 22A-7

Implement Strong Access Control Measures

Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know

Sections

7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood.

7.2 Access to system components and data is appropriately defined and assigned.

7.3 Access to system components and data is managed via an access control system(s).

Overview

Unauthorized individuals may gain access to critical data or systems due to ineffective access control rules and definitions. To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities.

“Access” or “access rights” are created by rules that provide users access to systems, applications, and data, while “privileges” allow a user to perform a specific action or function in relation to that system, application, or data. For example, a user may have access rights to specific data, but whether they can only read that data, or can also change or delete the data is determined by the user’s assigned privileges.

“Need to know” refers to providing access to only the least amount of data needed to perform a job.

“Least privileges” refers to providing only the minimum level of privileges needed to perform a job.

These requirements apply to user accounts and access for employees, contractors, consultants, and internal and external vendors and other third parties (for example, for providing support or maintenance services). Certain requirements also apply to application and system accounts used by the entity (also called “service accounts”).

These requirements do not apply to consumers (cardholders).

Refer to *Appendix G* for definitions of PCI DSS terms.

Exhibit 22A-7

Requirements and Testing Procedures		Guidance
7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Requirement 7.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 7. While it is important to define the specific policies or procedures called out in Requirement 7, it is equally important to ensure they are properly documented, maintained, and disseminated. **Good Practice** It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle. **Definitions** Security policies define the entity's security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives.
7.1.1 All security policies and operational procedures that are identified in Requirement 7 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	**7.1.1** Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 7 are managed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Expectations, controls, and oversight for meeting activities within Requirement 7 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.		

Exhibit 22A-7

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities, and critical activities may not occur. **Good Practice** Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities. **Examples** A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).
7.1.2 Roles and responsibilities for performing activities in Requirement 7 are documented, assigned, and understood.	**7.1.2.a** Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 7 are documented and assigned.	
	7.1.2.b Interview personnel with responsibility for performing activities in Requirement 7 to verify that roles and responsibilities are assigned as and are understood.	
Customized Approach Objective		
Day-to-day responsibilities for performing all the activities in Requirement 7 are allocated. Personnel are accountable for successful, continuous operation of these requirements.		

Exhibit 22A-7

Requirements and Testing Procedures		Guidance
7.2 Access to system components and data is appropriately defined and assigned.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Defining an access control model that is appropriate for the entity's technology and access control philosophy supports a consistent and uniform way of allocating access and reduces the possibility of errors such as the granting of excessive rights. **Good Practice** A factor to consider when defining access needs is the separation of duties principle. This principle is intended to prevent fraud and misuse or theft of resources. For example, 1) dividing mission-critical functions and information system support functions among different individuals and/or functions, 2) establishing roles such that information system support activities are performed by different functions/individuals (for example, system management, programming, configuration management, quality assurance and testing, and network security), and 3) ensuring security personnel administering access control functions do not also administer audit functions. In environments where one individual performs multiple functions, such as administration and security operations, duties may be assigned so that no single individual has end-to-end control of a process without an independent checkpoint. For example, responsibility for configuration and responsibility for approving changes could be assigned to separate individuals. *(continued on next page)*
7.2.1 An access control model is defined and includes granting access as follows: • Appropriate access depending on the entity's business and access needs. • Access to system components and data resources that is based on users' job classification and functions. • The least privileges required (for example, user, administrator) to perform a job function.	**7.2.1.a** Examine documented policies and procedures and interview personnel to verify the access control model is defined in accordance with all elements specified in this requirement.	
	7.2.1.b Examine access control model settings and verify that access needs are appropriately defined in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Access requirements are established according to job functions following least-privilege and need-to-know principles.		

Exhibit 22A-7

Requirements and Testing Procedures		Guidance
7.1.2 *(continued)*		**Definitions** Key elements of an access control model include: • Resources to be protected (the systems/devices/data to which access is needed), • Job functions that need access to the resource (for example, system administrator, call-center personnel, store clerk), and • Which activities each job function needs to perform (for example, read/write or query). Once job functions, resources, and activities per job functions are defined, individuals can be granted access accordingly. **Examples** Access control models that entities can consider include role-based access control (RBAC) and attribute-based access control (ABAC). The access control model used by a given entity depends on their business and access needs.

Exhibit 22A-7

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	
7.2.2 Access is assigned to users, including privileged users, based on: • Job classification and function. • Least privileges necessary to perform job responsibilities.	**7.2.2.a** Examine policies and procedures to verify they cover assigning access to users in accordance with all elements specified in this requirement.	**Purpose** Assigning least privileges helps prevent users without sufficient knowledge about the application from incorrectly or accidentally changing application configuration or altering its security settings. Enforcing least privilege also helps to minimize the scope of damage if an unauthorized person gains access to a user ID. **Good Practice** Access rights are granted to a user by assignment to one or several functions. Access is assigned depending on the specific user functions and with the minimum scope required for the job. When assigning privileged access, it is important to assign individuals only the privileges they need to perform their job (the “least privileges”). For example, the database administrator or backup administrator should not be assigned the same privileges as the overall systems administrator. Once needs are defined for user functions (per PCI DSS requirement 7.2.1), it is easy to grant individuals access according to their job classification and function by using the already-created roles. Entities may wish to consider use of Privileged Access Management (PAM), which is a method to grant access to privileged accounts only when those privileges are required, immediately revoking that access once they are no longer needed.
	7.2.2.b Examine user access settings, including for privileged users, and interview responsible management personnel to verify that privileges assigned are in accordance with all elements specified in this requirement.	
Customized Approach Objective	**7.2.2.c** Interview personnel responsible for assigning access to verify that privileged user access is assigned in accordance with all elements specified in this requirement.	
Access to systems and data is limited to only the access needed to perform job functions, as defined in the related access roles.		

Exhibit 22A-7

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Documented approval (for example, in writing or electronically) assures that those with access and privileges are known and authorized by management, and that their access is necessary for their job function.
7.2.3 Required privileges are approved by authorized personnel.	**7.2.3.a** Examine policies and procedures to verify they define processes for approval of all privileges by authorized personnel.	
	7.2.3.b Examine user IDs and assigned privileges, and compare with documented approvals to verify that: • Documented approval exists for the assigned privileges. • The approval was by authorized personnel. • Specified privileges match the roles assigned to the individual.	
Customized Approach Objective		
Access privileges cannot be granted to users without appropriate, documented authorization.		

Exhibit 22A-7

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Regular review of access rights helps to detect excessive access rights remaining after user job responsibilities change, system functions change, or other modifications. If excessive user rights are not revoked in due time, they may be used by malicious users for unauthorized access. This review provides another opportunity to ensure that accounts for all terminated users have been removed (if any were missed at the time of termination), as well as to ensure that any third parties that no longer need access have had their access terminated. **Good Practice** When a user transfers into a new role or a new department, typically the privileges and access associated with their former role are no longer required. Continued access to privileges or functions that are no longer required may introduce the risk of misuse or errors. Therefore, when responsibilities change, processes that revalidate access help to ensure user access is appropriate for the user's new responsibilities. Entities can consider implementing a regular, repeatable process for conducting reviews of access rights, and assigning "data owners" that are responsible for managing and monitoring access to data related to their job function and that also ensure user access remains current and appropriate. As an example, a direct manager could review team access monthly, while the senior manager reviews their groups' access quarterly, both making updates to access as needed. The intent of these best practices is to support and facilitate conducting the reviews at least once every 6 months.
7.2.4 All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows: • At least once every six months. • To ensure user accounts and access remain appropriate based on job function. • Any inappropriate access is addressed. • Management acknowledges that access remains appropriate.	**7.2.4.a** Examine policies and procedures to verify they define processes to review all user accounts and related access privileges, including third-party/vendor accounts, in accordance with all elements specified in this requirement. **7.2.4.b** Interview responsible personnel and examine documented results of periodic reviews of user accounts to verify that all the results are in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Account privilege assignments are verified periodically by management as correct, and nonconformities are remediated.		
Applicability Notes		
This requirement applies to all user accounts and related access privileges, including those used by personnel and third parties/vendors, and accounts used to access third-party cloud services. See Requirements 7.2.5 and 7.2.5.1 and 8.6.1 through 8.6.3 for controls for application and system accounts. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

Exhibit 22A-7

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** It is important to establish the appropriate access level for application or system accounts. If such accounts are compromised, malicious users will receive the same access level as that granted to the application or system. Therefore, it is important to ensure limited access is granted to system and application accounts on the same basis as to user accounts. **Good Practice** Entities may want to consider establishing a baseline when setting up these application and system accounts including the following as applicable to the organization: • Making sure that the account is not a member of a privileged group such as domain administrators, local administrators, or root. • Restricting which computers the account can be used on. • Restricting hours of use. • Removing any additional settings like VPN access and remote access.
7.2.5 All application and system accounts and related access privileges are assigned and managed as follows: • Based on the least privileges necessary for the operability of the system or application. • Access is limited to the systems, applications, or processes that specifically require their use.	**7.2.5.a** Examine policies and procedures to verify they define processes to manage and assign application and system accounts and related access privileges in accordance with all elements specified in this requirement.	
	7.2.5.b Examine privileges associated with system and application accounts and interview responsible personnel to verify that application and system accounts and related access privileges are assigned and managed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Access rights granted to application and system accounts are limited to only the access needed for the operability of that application or system.		
Applicability Notes		
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.		

Exhibit 22A-7

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Regular review of access rights helps to detect excessive access rights remaining after system functions change, or other application or system modifications occur. If excessive rights are not removed when no longer needed, they may be used by malicious users for unauthorized access.
7.2.5.1 All access by application and system accounts and related access privileges are reviewed as follows: • Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1). • The application/system access remains appropriate for the function being performed. • Any inappropriate access is addressed. • Management acknowledges that access remains appropriate.	**7.2.5.1.a** Examine policies and procedures to verify they define processes to review all application and system accounts and related access privileges in accordance with all elements specified in this requirement.	
	7.2.5.1.b Examine the entity's targeted risk analysis for the frequency of periodic reviews of application and system accounts and related access privileges to verify the risk analysis was performed in accordance with all elements specified in Requirement 12.3.1.	
Customized Approach Objective	**7.2.5.1.c** Interview responsible personnel and examine documented results of periodic reviews of system and application accounts and related privileges to verify that the reviews occur in accordance with all elements specified in this requirement.	
Application and system account privilege assignments are verified periodically by management as correct, and nonconformities are remediated.		
Applicability Notes		
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.		

Exhibit 22A-7

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** The misuse of query access to repositories of cardholder data has been a regular cause of data breaches. Limiting such access to administrators reduces the risk of such access being abused by unauthorized users. **Definitions** "Programmatic methods" means granting access through means such as database stored procedures that allow users to perform controlled actions to data in a table, rather than via direct, unfiltered access to the data repository by end users (except for the responsible administrator(s), who need direct access to the database for their administrative duties). **Good Practice** Typical user actions include moving, copying, and deleting data. Also consider the scope of privilege needed when granting access. For example, access can be granted to specific objects such as data elements, files, tables, indexes, views, and stored routines. Granting access to repositories of cardholder data should follow the same process as all other granted access, meaning that it is based on roles, with only the privileges assigned to each user that are needed to perform their job functions.
7.2.6 All user access to query repositories of stored cardholder data is restricted as follows: • Via applications or other programmatic methods, with access and allowed actions based on user roles and least privileges. • Only the responsible administrator(s) can directly access or query repositories of stored CHD.	**7.2.6.a** Examine policies and procedures and interview personnel to verify processes are defined for granting user access to query repositories of stored cardholder data, in accordance with all elements specified in this requirement.	
	7.2.6.b Examine configuration settings for querying repositories of stored cardholder data to verify they are in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Direct unfiltered (ad hoc) query access to cardholder data repositories is prohibited, unless performed by an authorized administrator.		
Applicability Notes		
This requirement applies to controls for user access to query repositories of stored cardholder data. See Requirements 7.2.5 and 7.2.5.1 and 8.6.1 through 8.6.3 for controls for application and system accounts.		

Exhibit 22A-7

Requirements and Testing Procedures		Guidance
7.3 Access to system components and data is managed via an access control system(s).		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Without a mechanism to restrict access based on user's need to know, a user may unknowingly be granted access to cardholder data. Access control systems automate the process of restricting access and assigning privileges.
7.3.1 An access control system(s) is in place that restricts access based on a user's need to know and covers all system components.	**7.3.1** Examine vendor documentation and system settings to verify that access is managed for each system component via an access control system(s) that restricts access based on a user's need to know and covers all system components.	
Customized Approach Objective		
Access rights and privileges are managed via mechanisms intended for that purpose.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Restricting privileged access with an access control system reduces the opportunity for errors in the assignment of permissions to individuals, applications, and systems.
7.3.2 The access control system(s) is configured to enforce permissions assigned to individuals, applications, and systems based on job classification and function.	**7.3.2** Examine vendor documentation and system settings to verify that the access control system(s) is configured to enforce permissions assigned to individuals, applications, and systems based on job classification and function.	
Customized Approach Objective		
Individual account access rights and privileges to systems, applications, and data are only inherited from group membership.		

Exhibit 22A-7

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** A default setting of "deny all" ensures no one is granted access unless a rule is established specifically granting such access. **Good Practice** It is important to check the default configuration of access control systems because some are set by default to "allow all," thereby permitting access unless/until a rule is written to specifically deny it.
7.3.3 The access control system(s) is set to "deny all" by default.	**7.3.3** Examine vendor documentation and system settings to verify that the access control system(s) is set to "deny all" by default.	
Customized Approach Objective		
Access rights and privileges are prohibited unless expressly permitted.		

Exhibit 22A-8

Requirement 8: Identify Users and Authenticate Access to System Components

Sections

8.1 Processes and mechanisms for identifying users and authenticating access to system components are defined and understood.

8.2 User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.

8.3 Strong authentication for users and administrators is established and managed.

8.4 Multi-factor authentication (MFA) is implemented to secure access into the CDE.

8.5 Multi-factor authentication (MFA) systems are configured to prevent misuse.

8.6 Use of application and system accounts and associated authentication factors is strictly managed.

Overview

Two fundamental principles of identifying and authenticating users are to 1) establish the identity of an individual or process on a computer system, and 2) prove or verify the user associated with the identity is who the user claims to be.

Identification of an individual or process on a computer system is conducted by associating an identity with a person or process through an identifier, such as a user, system, or application ID. These IDs (also referred to as "accounts") fundamentally establish the identity of an individual or process by assigning unique identification to each person or process to distinguish one user or process from another. When each user or process can be uniquely identified, it ensures there is accountability for actions performed by that identity. When such accountability is in place, actions taken can be traced to known and authorized users and processes.

The element used to prove or verify the identity is known as the authentication factor. Authentication factors are 1) something you know, such as a password or passphrase, 2) something you have, such as a token device or smart card, or 3) something you are, such as a biometric element.

The ID and the authentication factor together are considered authentication credentials and are used to gain access to the rights and privileges associated with a user, application, system, or service accounts.

These requirements for identity and authentication are based on industry-accepted security principles and best practices to support the payment ecosystem. *NIST Special Publication 800-63, Digital Identity Guidelines* provides additional information on acceptable frameworks for digital identity and authentication factors. It is important to note that the *NIST Digital Identity Guidelines* is intended for US Federal Agencies and should be viewed in its entirety. Many of the concepts and approaches defined in these guidelines are expected to work with each other and not as standalone parameters.

Exhibit 22A-8

***Note**: Unless otherwise stated in the requirement, these requirements apply to **all accounts on all system components**, unless specifically called out in an individual requirement, including but not limited to:*

- *Point-of-sale accounts*
- *Accounts with administrative capabilities*
- *System and application accounts*
- *All accounts used to view or access cardholder data or to access systems with cardholder data.*

This includes accounts used by employees, contractors, consultants, internal and external vendors, and other third parties (for example, for providing support or maintenance services).

Certain requirements are not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction. When items do not apply, they are noted directly within the specific requirement.

These requirements do not apply to accounts used by consumers (cardholders).

Refer to Appendix G for definitions of PCI DSS terms.

Exhibit 22A-8

Requirements and Testing Procedures		Guidance
8.1 Processes and mechanisms for identifying users and authenticating access to system components are defined and understood.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Requirement 8.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 8. While it is important to define the specific policies or procedures called out in Requirement 8, it is equally important to ensure they are properly documented, maintained, and disseminated. **Good Practice** It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle. **Definitions** Security policies define the entity's security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives.
8.1.1 All security policies and operational procedures that are identified in Requirement 8 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	**8.1.1** Examine documentation and interview personnel to verify that security policies and operational procedures that are identified in Requirement 8 are managed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Expectations, controls, and oversight for meeting activities within Requirement 8 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.		

Exhibit 22A-8

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and critical activities may not occur. **Good Practice** Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities. **Examples** A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).
8.1.2 Roles and responsibilities for performing activities in Requirement 8 are documented, assigned, and understood.	**8.1.2.a** Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 8 are documented and assigned.	
	8.1.2.b Interview personnel with responsibility for performing activities in Requirement 8 to verify that roles and responsibilities are assigned as documented and are understood.	
Customized Approach Objective		
Day-to-day responsibilities for performing all the activities in Requirement 8 are allocated. Personnel are accountable for successful, continuous operation of these requirements.		

Exhibit 22A-8

Requirements and Testing Procedures		Guidance
8.2 User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** The ability to trace actions performed on a computer system to an individual establishes accountability and traceability and is fundamental to establishing effective access controls. By ensuring each user is uniquely identified, instead of using one ID for several employees, an organization can maintain individual responsibility for actions and an effective record in the audit log per employee. In addition, this will assist with issue resolution and containment when misuse or malicious intent occurs.
8.2.1 All users are assigned a unique ID before access to system components or cardholder data is allowed.	**8.2.1.a** Interview responsible personnel to verify that all users are assigned a unique ID for access to system components and cardholder data.	
	8.2.1.b Examine audit logs and other evidence to verify that access to system components and cardholder data can be uniquely identified and associated with individuals.	
Customized Approach Objective		
All actions by all users are attributable to an individual.		
Applicability Notes		
This requirement is not intended to apply to user accounts within point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction		

Exhibit 22A-8

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Group, shared, or generic (or default) IDs are typically delivered with software or operating systems—for example, root or with privileges associated with a specific function, such as an administrator. If multiple users share the same authentication credentials (for example, user ID and password), it becomes impossible to trace system access and activities to an individual. In turn, this prevents an entity from assigning accountability for, or having effective logging of, an individual's actions since a given action could have been performed by anyone in the group with knowledge of the user ID and associated authentication factors. The ability to associate individuals to the actions performed with an ID is essential to provide individual accountability and traceability regarding who performed an action, what action was performed, and when that action occurred. **Good Practice** If shared IDs are used for any reason, strong management controls need to be established to maintain individual accountability and traceability. *(continued on next page)*
8.2.2 Group, shared, or generic IDs, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows: • ID use is prevented unless needed for an exceptional circumstance. • Use is limited to the time needed for the exceptional circumstance. • Business justification for use is documented. • Use is explicitly approved by management. • Individual user identity is confirmed before access to an account is granted. • Every action taken is attributable to an individual user.	**8.2.2.a** Examine user account lists on system components and applicable documentation to verify that shared authentication credentials are only used when necessary, on an exception basis, and are managed in accordance with all elements specified in this requirement.	
	8.2.2.b Examine authentication policies and procedures to verify processes are defined for shared authentication credentials such that they are only used when necessary, on an exception basis, and are managed in accordance with all elements specified in this requirement.	
	8.2.2.c Interview system administrators to verify that shared authentication credentials are only used when necessary, on an exception basis, and are managed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
All actions performed by users with group, shared, or generic IDs are attributable to an individual person.		
Applicability Notes		
This requirement is not intended to apply to user accounts within point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction.		

Exhibit 22A-8

Requirements and Testing Procedures		Guidance
8.2.2 *(continued)*		**Examples** Tools and techniques can facilitate both management and security of these types of accounts and confirm individual user identity before access to an account is granted. Entities can consider password vaults or other system-managed controls such as the *sudo* command. An example of an exceptional circumstance is where all other authentication methods have failed, and a shared ID is needed for emergency use or "break the glass" administrator access.
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Service providers with remote access to customer premises typically use this access to support POS POI systems or provide other remote services. If a service provider uses the same authentication factors to access multiple customers, all the service provider's customers can easily be compromised if an attacker compromises that one factor. Criminals know this and deliberately target service providers looking for a shared authentication factor that gives them remote access to many merchants via that single factor. *(continued on next page)*
8.2.3 ***Additional requirement for service providers only:*** Service providers with remote access to customer premises use unique authentication factors for each customer premises.	**8.2.3** ***Additional testing procedure for service provider assessments only:*** Examine authentication policies and procedures and interview personnel to verify that service providers with remote access to customer premises use unique authentication factors for remote access to each customer premises.	
Customized Approach Objective		
A service provider's credential used for one customer cannot be used for any other customer.		

Exhibit 22A-8

Requirements and Testing Procedures		Guidance
Applicability Notes This requirement applies only when the entity being assessed is a service provider. This requirement is not intended to apply to service providers accessing their own shared services environments, where multiple customer environments are hosted. If service provider employees use shared authentication factors to remotely access customer premises, these factors must be unique per customer and managed in accordance with Requirement 8.2.2.		**Examples** Technologies such as multi-factor mechanisms that provide a unique credential for each connection (such as a single-use password) could also meet the intent of this requirement.

Exhibit 22A-8

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** It is imperative that the lifecycle of a user ID (additions, deletions, and modifications) is controlled so that only authorized accounts can perform functions, actions are auditable, and privileges are limited to only what is required. Attackers often compromise an existing account and then escalate the privileges of that account to perform unauthorized acts, or they may create new IDs to continue their activity in the background. It is essential to detect and respond when user IDs are created or changed outside the normal change process or without corresponding authorization.
8.2.4 Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows: • Authorized with the appropriate approval. • Implemented with only the privileges specified on the documented approval.	**8.2.4** Examine documented authorizations across various phases of the account lifecycle (additions, modifications, and deletions) and examine system settings to verify the activity has been managed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Lifecycle events for user IDs and authentication factors cannot occur without appropriate authorization.		
Applicability Notes		
This requirement applies to all user accounts, including employees, contractors, consultants, temporary workers, and third-party vendors.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If an employee or third party/vendor has left the company and still has access to the network via their user account, unnecessary or malicious access to cardholder data could occur—either by the former employee or by a malicious user who exploits the old and/or unused account.
8.2.5 Access for terminated users is immediately revoked.	**8.2.5.a** Examine information sources for terminated users and review current user access lists—for both local and remote access—to verify that terminated user IDs have been deactivated or removed from the access lists.	
	8.2.5.b Interview responsible personnel to verify that all physical authentication factors—such as, smart cards, tokens, etc.—have been returned or deactivated for terminated users.	
Customized Approach Objective		
The accounts of terminated users cannot be used.		

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Accounts that are not used regularly are often targets of attack since it is less likely that any changes, such as a changed password, will be noticed. As such, these accounts may be more easily exploited and used to access cardholder data. **Good Practice** Where it may be reasonably anticipated that an account will not be used for an extended period of time, such as an extended leave of absence, the account should be disabled as soon as the leave begins, rather than waiting 90 days.
8.2.6 Inactive user accounts are removed or disabled within 90 days of inactivity.	**8.2.6** Examine user accounts and last logon information, and interview personnel to verify that any inactive user accounts are removed or disabled within 90 days of inactivity.	
Customized Approach Objective		
Inactive user accounts cannot be used.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Allowing third parties to have 24/7 access into an entity's systems and networks in case they need to provide support increases the chances of unauthorized access. This access could result in an unauthorized user in the third party's environment or a malicious individual using the always-available external entry point into an entity's network. Where third parties do need access 24/7, it should be documented, justified, monitored, and tied to specific service reasons. *(continued on next page)*
8.2.7 Accounts used by third parties to access, support, or maintain system components via remote access are managed as follows: • Enabled only during the time period needed and disabled when not in use. • Use is monitored for unexpected activity.	**8.2.7** Interview personnel, examine documentation for managing accounts, and examine evidence to verify that accounts used by third parties for remote access are managed according to all elements specified in this requirement.	

Exhibit 22A-8

Requirements and Testing Procedures		Guidance
Customized Approach Objective Third-party remote access cannot be used except where specifically authorized and use is overseen by management.		**Good Practice** Enabling access only for the time periods needed and disabling it as soon as it is no longer required helps prevent misuse of these connections. Additionally, consider assigning third parties a start and stop date for their access in accordance with their service contract. Monitoring third-party access helps ensure that third parties are accessing only the systems necessary and only during approved time frames. Any unusual activity using third-party accounts should be followed up and resolved.

Exhibit 22A-8

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** When users walk away from an open machine with access to system components or cardholder data, there is a risk that the machine may be used by others in the user's absence, resulting in unauthorized account access and/or misuse. **Good Practice** The re-authentication can be applied either at the system level to protect all sessions running on that machine or at the application level. Entities may also want to consider staging controls in succession to further restrict the access of an unattended session as time passes. For example, the screensaver may activate after 15 minutes and log off the user after an hour. However, timeout controls must balance the risk of access and exposure with the impact to the user and purpose of the access. If a user needs to run a program from an unattended computer, the user can log in to the computer to initiate the program, and then "lock" the computer so that no one else can use the user's login while the computer is unattended. **Examples** One way to meet this requirement is to configure an automated screensaver to launch whenever the console is idle for 15 minutes and requiring the logged-in user to enter their password to unlock the screen.
8.2.8 If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session.	**8.2.8** Examine system configuration settings to verify that system/session idle timeout features for user sessions have been set to 15 minutes or less.	
Customized Approach Objective		
A user session cannot be used except by the authorized user.		
Applicability Notes		
This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction. This requirement is not meant to prevent legitimate activities from being performed while the console/PC is unattended.		

Exhibit 22A-8

Requirements and Testing Procedures		Guidance
8.3 Strong authentication for users and administrators is established and managed.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** When used in addition to unique IDs, an authentication factor helps protect user IDs from being compromised, since the attacker needs to have the unique ID and compromise the associated authentication factor(s). **Good Practice** A common approach for a malicious individual to compromise a system is to exploit weak or nonexistent authentication factors (for example, passwords/passphrases). Requiring strong authentication factors helps protect against this attack. **Further Information** See *fidoalliance.org* for more information about using tokens, smart cards, or biometrics as authentication factors.
8.3.1 All user access to system components for users and administrators is authenticated via at least one of the following authentication factors: • Something you know, such as a password or passphrase. • Something you have, such as a token device or smart card. • Something you are, such as a biometric element.	**8.3.1.a** Examine documentation describing the authentication factor(s) used to verify that user access to system components is authenticated via at least one authentication factor specified in this requirement.	
	8.3.1.b For each type of authentication factor used with each type of system component, observe an authentication to verify that authentication is functioning consistently with documented authentication factor(s).	
Customized Approach Objective		
An account cannot be accessed except with a combination of user identity and an authentication factor.		
Applicability Notes		
This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction. This requirement does not supersede multi-factor authentication (MFA) requirements but applies to those in-scope systems not otherwise subject to MFA requirements. A digital certificate is a valid option for "something you have" if it is unique for a particular user.		

Exhibit 22A-8

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
8.3.2 Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components.	**8.3.2.a** Examine vendor documentation and system configuration settings to verify that authentication factors are rendered unreadable with strong cryptography during transmission and storage.	Network devices and applications have been known to transmit unencrypted, readable authentication factors (such as passwords and passphrases) across the network and/or store these values without encryption. As a result, a malicious individual can easily intercept this information during transmission using a "sniffer," or directly access unencrypted authentication factors in files where they are stored, and then use this data to gain unauthorized access.
	8.3.2.b Examine repositories of authentication factors to verify that they are unreadable during storage.	
Customized Approach Objective	**8.3.2.c** Examine data transmissions to verify that authentication factors are unreadable during transmission.	
Cleartext authentication factors cannot be obtained, derived, or reused from the interception of communications or from stored data.		

Exhibit 22A-8

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Malicious individuals use "social engineering" techniques to impersonate a user of a system — for example, calling a help desk and acting as a legitimate user—to have an authentication factor changed so they can use a valid user ID. Requiring positive identification of a user reduces the probability of this type of attack succeeding. **Good Practice** Modifications to authentication factors for which user identity should be verified include but are not limited to performing password resets, provisioning new hardware or software tokens, and generating new keys. **Examples** Methods to verify a user’s identity include a secret question/answer, knowledge-based information, and calling the user back at a known and previously established phone number.
8.3.3 User identity is verified before modifying any authentication factor.	**8.3.3** Examine procedures for modifying authentication factors and observe security personnel to verify that when a user requests a modification of an authentication factor, the user’s identity is verified before the authentication factor is modified.	
Customized Approach Objective		
Unauthorized individuals cannot gain system access by impersonating the identity of an authorized user.		

Exhibit 22A-8

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Without account-lockout mechanisms in place, an attacker can continually try to guess a password through manual or automated tools (for example, password cracking) until the attacker succeeds and gains access to a user's account. If an account is locked out due to someone continually trying to guess a password, controls to delay reactivation of the locked account stop the malicious individual from guessing the password, as they will have to stop for a minimum of 30 minutes until the account is reactivated. **Good Practice** Before reactivating a locked account, the user's identity should be confirmed. For example, the administrator or help desk personnel can validate that the actual account owner is requesting reactivation, or there may be password reset self-service mechanisms that the account owner uses to verify their identity.
8.3.4 Invalid authentication attempts are limited by: • Locking out the user ID after not more than 10 attempts. • Setting the lockout duration to a minimum of 30 minutes or until the user's identity is confirmed.	**8.3.4.a** Examine system configuration settings to verify that authentication parameters are set to require that user accounts be locked out after not more than 10 invalid logon attempts. **8.3.4.b** Examine system configuration settings to verify that password parameters are set to require that once a user account is locked out, it remains locked for a minimum of 30 minutes or until the user's identity is confirmed.	
Customized Approach Objective		
An authentication factor cannot be guessed in a brute force, online attack.		
Applicability Notes		
This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If the same password/passphrase is used for every new user, an internal user, former employee, or malicious individual may know or easily discover the value and use it to gain access to accounts before the authorized user attempts to use the password.
8.3.5 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows: • Set to a unique value for first-time use and upon reset. • Forced to be changed immediately after the first use.	**8.3.5** Examine procedures for setting and resetting passwords/passphrases (if used as authentication factors to meet Requirement 8.3.1) and observe security personnel to verify that passwords/passphrases are set and reset in accordance with all elements specified in this requirement.	
Customized Approach Objective		
An initial or reset password/passphrase assigned to a user cannot be used by an unauthorized user.		

Exhibit 22A-8

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Strong passwords/passphrases may be the first line of defense into a network since a malicious individual will often first try to find accounts with weak, static, or non-existent passwords. If passwords are short or easily guessable, it is relatively easy for a malicious individual to find these weak accounts and compromise a network under the guise of a valid user ID. **Good Practice** Password/passphrase strength is dependent on password/passphrase complexity, length, and randomness. Passwords/passphrases should be sufficiently complex, so they are impractical for an attacker to guess or otherwise discover its value. Entities can consider adding increased complexity by requiring the use of special characters and upper- and lower-case characters, in addition to the minimum standards outlined by this requirement. Additional complexity increases the time required for offline brute force attacks of hashed passwords/passphrases. Another option for increasing the resistance of passwords to guessing attacks is by comparing proposed password/passphrases to a bad password list and having users provide new passwords for any passwords found on the list.
8.3.6 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity: • A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters). • Contain both numeric and alphabetic characters.	**8.3.6** Examine system configuration settings to verify that user password/passphrase complexity parameters are set in accordance with all elements specified in this requirement.	
Customized Approach Objective		
A guessed password/passphrase cannot be verified by either an online or offline brute force attack.		
Applicability Notes		
This requirement is not intended to apply to: • User accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction. • Application or system accounts, which are governed by requirements in section 8.6. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.* Until 31 March 2025, passwords must be a minimum length of seven characters in accordance with PCI DSS v3.2.1 Requirement 8.2.3.		

Exhibit 22A-8

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If password history is not maintained, the effectiveness of changing passwords is reduced, as previous passwords can be reused over and over. Requiring that passwords cannot be reused for a period reduces the likelihood that passwords that have been guessed or brute-forced will be re-used in the future. Passwords or passphrases may have previously been changed due to suspicion of compromise or because the password or passphrase exceeded its effective use period, both of which are reasons why previously used passwords should not be reused.
8.3.7 Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used.	**8.3.7** Examine system configuration settings to verify that password parameters are set to require that new passwords/passphrases cannot be the same as the four previously used passwords/passphrases.	
Customized Approach Objective		
A previously used password cannot be used to gain access to an account for at least 12 months.		
Applicability Notes		
This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction.		

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Communicating authentication policies and procedures to all users helps them to understand and abide by the policies. **Good Practice** Guidance on selecting strong passwords may include suggestions to help personnel select hard-to-guess passwords that do not contain dictionary words or information about the user, such as the user ID, names of family members, date of birth, etc. Guidance for protecting authentication factors may include not writing down passwords or not saving them in insecure files, and being alert to malicious individuals who may try to exploit their passwords (for example, by calling an employee and asking for their password so the caller can “troubleshoot a problem”). Alternatively, entities can implement processes to confirm passwords meet password policy, for example, by comparing password choices to a list of unacceptable passwords and having users choose a new password for any that match with one on the list. Instructing users to change passwords if there is a chance the password is no longer secure can prevent malicious users from using a legitimate password to gain unauthorized access.
8.3.8 Authentication policies and procedures are documented and communicated to all users including: • Guidance on selecting strong authentication factors. • Guidance for how users should protect their authentication factors. • Instructions not to reuse previously used passwords/passphrases. • Instructions to change passwords/passphrases if there is any suspicion or knowledge that the password/passphrases have been compromised and how to report the incident.	**8.3.8.a** Examine procedures and interview personnel to verify that authentication policies and procedures are distributed to all users.	
	8.3.8.b Review authentication policies and procedures that are distributed to users and verify they include the elements specified in this requirement.	
	8.3.8.c Interview users to verify that they are familiar with authentication policies and procedures.	
Customized Approach Objective		
Users are knowledgeable about the correct use of authentication factors and can access assistance and guidance when required.		

Exhibit 22A-8

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Access to in-scope system components that are not in the CDE may be provided using a single authentication factor, such as a password/passphrase, token device or smart card, or biometric attribute. Where passwords/passphrases are employed as the only authentication factor for such access, additional controls are required to protect the integrity of the password/passphrase. **Good Practice** Passwords/passphrases that are valid for a long time without a change provide malicious individuals with more time to break the password/phrase. Periodically changing passwords offers less time for a malicious individual to crack a password/passphrase and less time to use a compromised password. Using a password/passphrase as the only authentication factor provides a single point of failure if compromised. Therefore, in these implementations, controls are needed to minimize how long malicious activity could occur via a compromised password/passphrase. *(continued on next page)*
8.3.9 If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either: • Passwords/passphrases are changed at least once every 90 days, **OR** • The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.	**8.3.9** If passwords/passphrases are used as the only authentication factor for user access, inspect system configuration settings to verify that passwords/passphrases are managed in accordance with ONE of the elements specified in this requirement.	
Customized Approach Objective		
An undetected compromised password/passphrase cannot be used indefinitely.		
Applicability Notes		
This requirement does not apply to in-scope system components where MFA is used. This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction. This requirement does not apply to service providers' customer accounts but does apply to accounts for service provider personnel.		

Exhibit 22A-8

Requirements and Testing Procedures		Guidance
8.3.9 *(continued)*		Dynamically analyzing an account's security posture is another option that allows for more rapid detection and response to address potentially compromised credentials. Such analysis takes a number of data points, which may include device integrity, location, access times, and the resources accessed to determine in real time whether an account can be granted access to a requested resource. In this way, access can be denied and accounts blocked if it is suspected that authentication credentials have been compromised. **Further Information** For information about using dynamic analysis to manage user access to resources, see *NIST SP 800-207 Zero Trust Architecture*.

Exhibit 22A-8

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Using a password/passphrase as the only authentication factor provides a single point of failure if compromised. Therefore, in these implementations, controls are needed to minimize how long malicious activity could occur via a compromised password/passphrase. **Good Practice** Passwords/passphrases that are valid for a long time without a change provide malicious individuals with more time to break the password/phrase. Periodically changing passwords offers less time for a malicious individual to crack a password/passphrase and less time to use a compromised password.
8.3.10 *Additional requirement for service providers only:* If passwords/passphrases are used as the only authentication factor for customer user access to cardholder data (i.e., in any single-factor authentication implementation), then guidance is provided to customer users including: • Guidance for customers to change their user passwords/passphrases periodically. • Guidance as to when, and under what circumstances, passwords/passphrases are to be changed.	**8.3.10 *Additional testing procedure for service provider assessments only:*** If passwords/passphrases are used as the only authentication factor for customer user access to cardholder data, examine guidance provided to customer users to verify that the guidance includes all elements specified in this requirement.	
Customized Approach Objective		
Passwords/passphrases for service providers' customers cannot be used indefinitely.		
Applicability Notes		
This requirement applies only when the entity being assessed is a service provider. This requirement does not apply to accounts of consumer users accessing their own payment card information. *This requirement for service providers will be superseded by Requirement 8.3.10.1 once 8.3.10.1 becomes effective.*		

Exhibit 22A-8

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Using a password/passphrase as the only authentication factor provides a single point of failure if compromised. Therefore, in these implementations, controls are needed to minimize how long malicious activity could occur via a compromised password/passphrase. **Good Practice** Passwords/passphrases that are valid for a long time without a change provide malicious individuals with more time to break the password/phrase. Periodically changing passwords offers less time for a malicious individual to crack a password/passphrase and less time to use a compromised password. Dynamically analyzing an account's security posture is another option that allows for more rapid detection and response to address potentially compromised credentials. Such analysis takes a number of data points which may include device integrity, location, access times, and the resources accessed to determine in real time whether an account can be granted access to a requested resource. In this way, access can be denied and accounts blocked if it is suspected that account credentials have been compromised. **Further Information** For information about using dynamic analysis to manage user access to resources, refer to *NIST SP 800-207 Zero Trust Architecture*.
8.3.10.1 ***Additional requirement for service providers only:*** If passwords/passphrases are used as the only authentication factor for customer user access (i.e., in any single-factor authentication implementation) then either: • Passwords/passphrases are changed at least once every 90 days, **OR** • The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.	**8.3.10.1** ***Additional testing procedure for service provider assessments only:*** If passwords/passphrases are used as the only authentication factor for customer user access, inspect system configuration settings to verify that passwords/passphrases are managed in accordance with ONE of the elements specified in this requirement.	
Customized Approach Objective		
Passwords/passphrases for service providers' customers cannot be used indefinitely.		
Applicability Notes		
This requirement applies only when the entity being assessed is a service provider. This requirement does not apply to accounts of consumer users accessing their own payment card information. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.* Until this requirement is effective on 31 March 2025, service providers may meet either Requirement 8.3.10 or 8.3.10.1.		

Exhibit 22A-8

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If multiple users can use authentication factors such as tokens, smart cards, and certificates, it may be impossible to identify the individual using the authentication mechanism. **Good Practice** Having physical and/or logical controls (for example, a PIN, biometric data, or a password) to uniquely authenticate the user of the account will prevent unauthorized users from gaining access to the user account through use of a shared authentication factor.
8.3.11 Where authentication factors such as physical or logical security tokens, smart cards, or certificates are used: • Factors are assigned to an individual user and not shared among multiple users. • Physical and/or logical controls ensure only the intended user can use that factor to gain access.	**8.3.11.a** Examine authentication policies and procedures to verify that procedures for using authentication factors such as physical security tokens, smart cards, and certificates are defined and include all elements specified in this requirement.	
	8.3.11.b Interview security personnel to verify authentication factors are assigned to an individual user and not shared among multiple users.	
Customized Approach Objective An authentication factor cannot be used by anyone other than the user to which it is assigned.	**8.3.11.c** Examine system configuration settings and/or observe physical controls, as applicable, to verify that controls are implemented to ensure only the intended user can use that factor to gain access.	

Exhibit 22A-8

Requirements and Testing Procedures		Guidance
8.4 Multi-factor authentication (MFA) is implemented to secure access into the CDE.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Requiring more than one type of authentication factor reduces the probability that an attacker can gain access to a system by masquerading as a legitimate user, because the attacker would need to compromise multiple authentication factors. This is especially true in environments where traditionally the single authentication factor employed was something a user knows such as a password or passphrase. **Good Practice** Implementing MFA for non-console administrative access to in-scope system components that are not part of the CDE will help prevent unauthorized users from using a single factor to gain access and compromise in-scope system components. **Definitions** Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication.
8.4.1 MFA is implemented for all non-console access into the CDE for personnel with administrative access.	**8.4.1.a** Examine network and/or system configurations to verify MFA is required for all non-console into the CDE for personnel with administrative access.	
	8.4.1.b Observe administrator personnel logging into the CDE and verify that MFA is required.	
Customized Approach Objective		
Administrative access to the CDE cannot be obtained by the use of a single authentication factor.		
Applicability Notes		
The requirement for MFA for non-console administrative access applies to all personnel with elevated or increased privileges accessing the CDE via a non-console connection—that is, via logical access occurring over a network interface rather than via a direct, physical connection.		

Exhibit 22A-8

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Requiring more than one type of authentication factor reduces the probability that an attacker can gain access to a system by masquerading as a legitimate user, because the attacker would need to compromise multiple authentication factors. This is especially true in environments where traditionally the single authentication factor employed was something a user knows such as a password or passphrase. *(continued on next page)*
8.4.2 MFA is implemented for all non-console access into the CDE.	**8.4.2.a** Examine network and/or system configurations to verify MFA is implemented for all non-console access into the CDE. **8.4.2.b** Observe personnel logging in to the CDE and examine evidence to verify that MFA is required.	
Customized Approach Objective		
Access into the CDE cannot be obtained by the use of a single authentication factor.		

Exhibit 22A-8

Requirements and Testing Procedures		Guidance
Applicability Notes This requirement does not apply to: • Application or system accounts performing automated functions. • User accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction. • User accounts that are only authenticated with phishing-resistant authentication factors. MFA is required for both types of access specified in Requirements 8.4.2 and 8.4.3. Therefore, applying MFA to one type of access does not replace the need to apply another instance of MFA to the other type of access. If an individual first connects to the entity's network via remote access, and then later initiates a connection into the CDE from within the network, per this requirement the individual would authenticate using MFA twice, once when connecting via remote access to the entity's network and once when connecting from the entity's network into the CDE. *(continued on next page)*		**Definitions** Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication. Refer to *Appendix G* for the definition of "phishing resistant authentication."

Exhibit 22A-8

Requirements and Testing Procedures		Guidance
The MFA requirements apply for all types of system components, including cloud, hosted systems, and on-premises applications, network security devices, workstations, servers, and endpoints, and includes access directly to an entity's networks or systems as well as web-based access to an application or function. MFA for access into the CDE can be implemented at the network or system/application level; it does not have to be applied at both levels. For example, if MFA is used when a user connects to the CDE network, it does not have to be used when the user logs into each system or application within the CDE. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

Exhibit 22A-8

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Requiring more than one type of authentication factor reduces the probability that an attacker can gain access to a system by masquerading as a legitimate user, because the attacker would need to compromise multiple authentication factors. This is especially true in environments where traditionally the single authentication factor employed was something a user knows, such as a password or passphrase. **Definitions** Multi-factor authentication (MFA) requires an individual to present a minimum of two of the three authentication factors specified in Requirement 8.3.1 before access is granted. Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication. *(continued on next page)*
8.4.3 MFA is implemented for all remote access originating from outside the entity's network that could access or impact the CDE.	**8.4.3.a** Examine network and/or system configurations for remote access servers and systems to verify MFA is required in accordance with all elements specified in this requirement. **8.4.3.b** Observe personnel (for example, users and administrators) and third parties connecting remotely to the network and verify that multi-factor authentication is required.	
Customized Approach Objective		
Remote access to the entity's network cannot be obtained by using a single authentication factor.		

Exhibit 22A-8

Requirements and Testing Procedures		Guidance
Applicability Notes		
The requirement for MFA for remote access originating from outside the entity’s network applies to all user accounts that can access the network remotely, where that remote access leads to or could lead to access into the CDE. This includes all remote access by personnel (users and administrators), and third parties (including, but not limited to, vendors, suppliers, service providers, and customers). If remote access is to a part of the entity’s network that is properly segmented from the CDE, such that remote users cannot access or impact the CDE, MFA for remote access to that part of the network is not required. However, MFA is required for any remote access to networks with access to the CDE and is recommended for all remote access to the entity’s networks. The MFA requirements apply for all types of system components, including cloud, hosted systems, and on-premises applications, network security devices, workstations, servers, and endpoints, and includes access directly to an entity’s networks or systems as well as web-based access to an application or function.		

Exhibit 22A-8

Requirements and Testing Procedures		Guidance
8.5 Multi-factor authentication (MFA) systems are configured to prevent misuse.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Poorly configured MFA systems can be bypassed by attackers. This requirement therefore addresses configuration of MFA system(s) that provide MFA for users accessing system components in the CDE. **Definitions** Using one type of factor twice (for example, using two separate passwords) is not considered multi-factor authentication. A replay attack is when an attacker intercepts a valid transmission of data and then resends or redirects this communication for malicious purposes. In MFA implementations, replay attacks are typically used to gain unauthorized access by leveraging legitimate credentials. **Examples** Examples of methods to help protect against replay attacks include, but are not limited to: • Unique session identifiers and session keys • Timestamps • Time-based, one-time passwords or passcodes • Anti-replay mechanisms that detect and reject duplicated authentication attempts. *(continued on next page)*
8.5.1 MFA systems are implemented as follows: • The MFA system is not susceptible to replay attacks. • MFA systems cannot be bypassed by any users, including administrative users unless specifically documented, and authorized by management on an exception basis, for a limited time period. • At least two different types of authentication factors are used. • Success of all authentication factors is required before access is granted.	**8.5.1.a** Examine vendor system documentation to verify that the MFA system is not susceptible to replay attacks. **8.5.1.b** Examine system configurations for the MFA implementation to verify it is configured in accordance with all elements specified in this requirement. **8.5.1.c** Interview responsible personnel and observe processes to verify that any requests to bypass MFA are specifically documented and authorized by management on an exception basis, for a limited time period. **8.5.1.d** Observe personnel logging into system components in the CDE to verify that access is granted only after all authentication factors are successful. **8.5.1.e** Observe personnel connecting remotely from outside the entity's network to verify that access is granted only after all authentication factors are successful.	
Customized Approach Objective		
MFA systems are resistant to attack and strictly control any administrative overrides.		

Exhibit 22A-8

Requirements and Testing Procedures		Guidance
Applicability Notes *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		**Further Information** For more information about MFA systems and features, refer to the following: PCI SSC's *Information Supplement: Multi-Factor Authentication* PCI SSC's Frequently Asked Questions (FAQs) on this topic.

Exhibit 22A-8

Requirements and Testing Procedures		Guidance
8.6 Use of application and system accounts and associated authentication factors is strictly managed.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Like individual user accounts, system and application accounts require accountability and strict management to ensure they are used only for the intended purpose and are not misused. Attackers often compromise system or application accounts to gain access to cardholder data. **Good Practice** Where possible, configure system and application accounts to disallow interactive login to prevent unauthorized individuals from logging in and using the account with its associated system privileges, and to limit the machines and devices on which the account can be used. **Definitions** Interactive login is the ability for a person to log into a system or application account in the same manner as a normal user account. Using system and application accounts this way means there is no accountability and traceability of actions taken by the user. Refer to *Appendix G* for the definition of “application and system accounts.”
8.6.1 If accounts used by systems or applications can be used for interactive login, they are managed as follows: • Interactive use is prevented unless needed for an exceptional circumstance. • Interactive use is limited to the time needed for the exceptional circumstance. • Business justification for interactive use is documented. • Interactive use is explicitly approved by management. • Individual user identity is confirmed before access to account is granted. • Every action taken is attributable to an individual user.	**8.6.1** Examine application and system accounts that can be used interactively and interview administrative personnel to verify that application and system accounts are managed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
When used interactively, all actions with accounts designated as system or application accounts are authorized and attributable to an individual person.		
Applicability Notes		
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.		

Exhibit 22A-8

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Not properly protecting passwords/passphrases used by application and system accounts, especially if those accounts can be used for interactive login, increases the risk and success of unauthorized use of those privileged accounts. **Good Practice** Changing these values due to suspected or confirmed disclosure can be particularly difficult to implement. Tools can facilitate both management and security of authentication factors for application and system accounts. For example, consider password vaults or other system-managed controls.
8.6.2 Passwords/passphrases for any application and system accounts that can be used for interactive login are not hard coded in scripts, configuration/property files, or bespoke and custom source code.	**8.6.2.a** Interview personnel and examine system development procedures to verify that processes are defined for application and system accounts that can be used for interactive login, specifying that passwords/passphrases are not hard coded in scripts, configuration/property files, or bespoke and custom source code.	
	8.6.2.b Examine scripts, configuration/property files, and bespoke and custom source code for application and system accounts that can be used for interactive login, to verify passwords/passphrases for those accounts are not present.	
Customized Approach Objective		
Passwords/passphrases used by application and system accounts cannot be used by unauthorized personnel.		
Applicability Notes		
Stored passwords/passphrases are required to be encrypted in accordance with PCI DSS Requirement 8.3.2. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

Exhibit 22A-8

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Systems and application accounts pose more inherent security risk than user accounts because they often run in an elevated security context, with access to systems that may not be typically granted to user accounts, such as programmatic access to databases, etc. As a result, special consideration must be made to protect passwords/passphrases used for application and system accounts. **Good Practice** Entities should consider the following risk factors when determining how to protect application and system passwords/passphrases against misuse: • How securely the passwords/passphrases are stored (for example, whether they are stored in a password vault). • Staff turnover. • The number of people with access to the authentication factor. • Whether the account can be used for interactive login. • Whether the security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly (see Requirement 8.3.9). All these elements affect the level of risk for application and system accounts and might impact the security of systems accessed by the system and application accounts. *(continued on next page)*
8.6.3 Passwords/passphrases for any application and system accounts are protected against misuse as follows: • Passwords/passphrases are changed periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1) and upon suspicion or confirmation of compromise. • Passwords/passphrases are constructed with sufficient complexity appropriate for how frequently the entity changes the passwords/passphrases.	**8.6.3.a** Examine policies and procedures to verify that procedures are defined to protect passwords/passphrases for application or system accounts against misuse in accordance with all elements specified in this requirement.	
	8.6.3.b Examine the entity's targeted risk analysis for the change frequency and complexity for passwords/passphrases for application and system accounts to verify the risk analysis was performed in accordance with all elements specified in Requirement 12.3.1 and addresses: • The frequency defined for periodic changes to application and system passwords/passphrases. • The complexity defined for passwords/passphrases and appropriateness of the complexity relative to the frequency of changes.	
Customized Approach Objective	**8.6.3.c** Interview responsible personnel and examine system configuration settings to verify that passwords/passphrases for any application and system accounts are protected against misuse in accordance with all elements specified in this requirement.	
Passwords/passphrases used by application and system accounts cannot be used indefinitely and are structured to resist brute-force and guessing attacks.		
Applicability Notes		
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.		

Exhibit 22A-8

Requirements and Testing Procedures		Guidance
8.6.3 *(continued)*		Entities should correlate their selected change frequency for application and system passwords/passwords with their selected complexity for those passwords/passphrases – i.e., the complexity should be more rigorous when passwords/passphrases are changed infrequently and can be less rigorous when changed more frequently. For example, a longer change frequency is more justifiable when passwords/passphrases complexity is set to 36 alphanumeric characters with upper- and lower-case letters, numbers, and special characters. Best practices are to consider password changes at least once a year, a password/passphrase length of at least 15 characters, and complexity for the passwords/passphrase of alphanumeric characters, with upper- and lower-case letters, and special characters. **Further Information** For information about variability and equivalency of password strength for passwords/passphrases of different formats, see the industry standards (for example, the current version of *NIST SP 800-63 Digital Identity Guidelines*).

Exhibit 22A-9

Requirement 9: Restrict Physical Access to Cardholder Data

Sections

9.1 Processes and mechanisms for restricting physical access to cardholder data are defined and understood.

9.2 Physical access controls manage entry into facilities and systems containing cardholder data.

9.3 Physical access for personnel and visitors is authorized and managed.

9.4 Media with cardholder data is securely stored, accessed, distributed, and destroyed.

9.5 Point of interaction (POI) devices are protected from tampering and unauthorized substitution.

Overview

Any physical access to cardholder data or systems that store, process, or transmit cardholder data provides the opportunity for individuals to access and/or remove systems or hardcopies containing cardholder data; therefore, physical access should be appropriately restricted.

There are three different areas mentioned in Requirement 9:

1. Requirements that specifically refer to sensitive areas are intended to apply to those areas only. Each entity should identify the sensitive areas in its environments to ensure the appropriate physical controls are implemented.
2. Requirements that specifically refer to the cardholder data environment (CDE) are intended to apply to the entire CDE, including any sensitive areas residing within the CDE.
3. Requirements that specifically refer to the facility are referencing the types of controls that may be managed more broadly at the physical boundary of a business premise (such as a building) within which CDEs and sensitive areas reside. These controls often exist outside a CDE or sensitive area, for example a guard desk that identifies, badges, and logs visitors. The term “facility” is used to recognize that these controls may exist at different places within a facility, for instance, at building entry or at an internal entrance to a data center or office space.

Refer to *Appendix G* for definitions of “media,” “personnel,” “sensitive areas,” “visitors,” and other PCI DSS terms.

Exhibit 22A-9

Requirements and Testing Procedures		Guidance
9.1 Processes and mechanisms for restricting physical access to cardholder data are defined and understood.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Requirement 9.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 9. While it is important to define the specific policies or procedures called out in Requirement 9, it is equally important to ensure they are properly documented, maintained, and disseminated. **Good Practice** It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle. **Definitions** Security policies define the entity's security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives. Policies and procedures, including updates, are actively communicated to all affected personnel, and are supported by operating procedures describing how to perform activities.
9.1.1 All security policies and operational procedures that are identified in Requirement 9 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	**9.1.1** Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 9 are managed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Expectations, controls, and oversight for meeting activities within Requirement 9 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.		

Exhibit 22A-9

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities, and critical activities may not occur. **Good Practice** Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities. A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).
9.1.2 Roles and responsibilities for performing activities in Requirement 9 are documented, assigned, and understood.	**9.1.2.a** Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 9 are documented and assigned.	
	9.1.2.b Interview personnel with responsibility for performing activities in Requirement 9 to verify that roles and responsibilities are assigned as documented and are understood.	
Customized Approach Objective		
Day-to-day responsibilities for performing all the activities in Requirement 9 are allocated. Personnel are accountable for successful, continuous operation of these requirements.		

Exhibit 22A-9

Requirements and Testing Procedures		Guidance
9.2 Physical access controls manage entry into facilities and systems containing cardholder data.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Without physical access controls, unauthorized persons could potentially gain access to the CDE and sensitive information, or could alter system configurations, introduce vulnerabilities into the network, or destroy or steal equipment. Therefore, the purpose of this requirement is that physical access to the CDE is controlled via physical security controls such as badge readers or other mechanisms such as lock and key. **Good Practice** Whichever mechanism meets this requirement, it must be sufficient for the organization to verify that only authorized personnel are granted access. **Examples** Facility entry controls include physical security controls at each computer room, data center, and other physical areas with systems in the CDE. It can also include badge readers or other devices that manage physical access controls, such as lock and key with a current list of all individuals holding the keys.
9.2.1 Appropriate facility entry controls are in place to restrict physical access to systems in the CDE.	**9.2.1** Observe entry controls and interview responsible personnel to verify that physical security controls are in place to restrict access to systems in the CDE.	
Customized Approach Objective		
System components in the CDE cannot be physically accessed by unauthorized personnel.		
Applicability Notes		
This requirement does not apply to locations that are publicly accessible by consumers (cardholders).		

Exhibit 22A-9

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	
9.2.1.1 Individual physical access to sensitive areas within the CDE is monitored with either video cameras or physical access control mechanisms (or both) as follows: • Entry and exit points to/from sensitive areas within the CDE are monitored. • Monitoring devices or mechanisms are protected from tampering or disabling. • Collected data is reviewed and correlated with other entries. • Collected data is stored for at least three months, unless otherwise restricted by law.	**9.2.1.1.a** Observe locations where individual physical access to sensitive areas within the CDE occurs to verify that either video cameras or physical access control mechanisms (or both) are in place to monitor the entry and exit points.	**Purpose** Maintaining details of individuals entering and exiting the sensitive areas can help with investigations of physical breaches by identifying individuals that physically accessed the sensitive areas, as well as when they entered and exited. **Good Practice** Whichever mechanism meets this requirement, it should effectively monitor all entry and exit points to sensitive areas. Criminals attempting to gain physical access to sensitive areas will often try to disable or bypass the monitoring controls. To protect these controls from tampering, video cameras could be positioned so they are out of reach and/or be monitored to detect tampering. Similarly, physical access control mechanisms could be monitored or have physical protections installed to prevent them from being damaged or disabled by malicious individuals.
	9.2.1.1.b Observe locations where individual physical access to sensitive areas within the CDE occurs to verify that either video cameras or physical access control mechanisms (or both) are protected from tampering or disabling.	
Customized Approach Objective	**9.2.1.1.c** Observe the physical access control mechanisms and/or examine video cameras and interview responsible personnel to verify that: • Collected data from video cameras and/or physical access control mechanisms is reviewed and correlated with other entries. • Collected data is stored for at least three months.	
Trusted, verifiable records are maintained of individual physical entry to, and exit from, sensitive areas.		

Exhibit 22A-9

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	
9.2.2 Physical and/or logical controls are implemented to restrict use of publicly accessible network jacks within the facility. **Customized Approach Objective** Unauthorized devices cannot connect to the entity's network from public areas within the facility.	**9.2.2** Interview responsible personnel and observe locations of publicly accessible network jacks to verify that physical and/or logical controls are in place to restrict access to publicly accessible network jacks within the facility.	**Purpose** Restricting access to network jacks (or network ports) will prevent malicious individuals from plugging into readily available network jacks and gaining access to the CDE or systems connected to the CDE. **Good Practice** Whether logical or physical controls, or a combination of both, are used, they should prevent an individual or device that is not explicitly authorized from being able to connect to the network. **Examples** Methods to meet this requirement include network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks.
Defined Approach Requirements	**Defined Approach Testing Procedures**	
9.2.3 Physical access to wireless access points, gateways, networking/communications hardware, and telecommunication lines within the facility is restricted. **Customized Approach Objective** Physical networking equipment cannot be accessed by unauthorized personnel.	**9.2.3** Interview responsible personnel and observe locations of hardware and lines to verify that physical access to wireless access points, gateways, networking/communications hardware, and telecommunication lines within the facility is restricted.	**Purpose** Without appropriate physical security over access to wireless components and devices, and computer networking and telecommunications equipment and lines, malicious users could gain access to the entity's network resources. Additionally, they could connect their own devices to the network to gain unauthorized access to the CDE or systems connected to the CDE. Additionally, securing networking and communications hardware prevents malicious users from intercepting network traffic or physically connecting their own devices to wired network resources.

Exhibit 22A-9

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Locking console login screens prevents unauthorized persons from gaining access to sensitive information, altering system configurations, introducing vulnerabilities into the network, or destroying records.
9.2.4 Access to consoles in sensitive areas is restricted via locking when not in use.	**9.2.4** Observe a system administrator's attempt to log into consoles in sensitive areas and verify that they are "locked" to prevent unauthorized use.	
Customized Approach Objective		
Physical consoles within sensitive areas cannot be used by unauthorized personnel.		

Exhibit 22A-9

Requirements and Testing Procedures		Guidance
9.3 Physical access for personnel and visitors is authorized and managed.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Establishing procedures for granting, managing, and removing access when it is no longer needed ensures non-authorized individuals are prevented from gaining access to areas containing cardholder data. In addition, it is important to limit access to the actual badging system and badging materials to prevent unauthorized personnel from making their own badges and/or setting up their own access rules. **Good Practice** It is important to visually identify the personnel that are physically present, and whether the individual is a visitor or an employee. **Definitions** Refer to *Appendix G* for the definition of "personnel." **Examples** One way to identify personnel is to assign them badges.
9.3.1 Procedures are implemented for authorizing and managing physical access of personnel to the CDE, including: • Identifying personnel. • Managing changes to an individual's physical access requirements. • Revoking or terminating personnel identification. • Limiting access to the identification process or system to authorized personnel.	**9.3.1.a** Examine documented procedures to verify that procedures to authorize and manage physical access of personnel to the CDE are defined in accordance with all elements specified in this requirement.	
	9.3.1.b Observe identification methods, such as ID badges, and processes to verify that personnel in the CDE are clearly identified.	
Customized Approach Objective	**9.3.1.c** Observe processes to verify that access to the identification process, such as a badge system, is limited to authorized personnel.	
Requirements for access to the physical CDE are defined and enforced to identify and authorize personnel.		

Exhibit 22A-9

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Controlling physical access to sensitive areas helps ensure that only authorized personnel with a legitimate business need are granted access. **Good Practice** Where possible, organizations should have policies and procedures to ensure that before personnel leaving the organization, all physical access mechanisms are returned, or disabled as soon as possible upon their departure. This will ensure personnel cannot gain physical access to sensitive areas once their employment has ended.
9.3.1.1 Physical access to sensitive areas within the CDE for personnel is controlled as follows: • Access is authorized and based on individual job function. • Access is revoked immediately upon termination. • All physical access mechanisms, such as keys, access cards, etc., are returned or disabled upon termination.	**9.3.1.1.a** Observe personnel in sensitive areas within the CDE, interview responsible personnel, and examine physical access control lists to verify that: • Access to the sensitive area is authorized. • Access is required for the individual's job function.	
	9.3.1.1.b Observe processes and interview personnel to verify that access of all personnel is revoked immediately upon termination.	
Customized Approach Objective	**9.3.1.1.c** For terminated personnel, examine physical access controls lists and interview responsible personnel to verify that all physical access mechanisms (such as keys, access cards, etc.) were returned or disabled.	
Sensitive areas cannot be accessed by unauthorized personnel.		

Exhibit 22A-9

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	
9.3.2 Procedures are implemented for authorizing and managing visitor access to the CDE, including: • Visitors are authorized before entering. • Visitors are escorted at all times. • Visitors are clearly identified and given a badge or other identification that expires. • Visitor badges or other identification visibly distinguishes visitors from personnel.	**9.3.2.a** Examine documented procedures and interview personnel to verify procedures are defined for authorizing and managing visitor access to the CDE in accordance with all elements specified in this requirement.	**Purpose** Visitor controls are important to reduce the ability of unauthorized and malicious persons to gain access to facilities and potentially to cardholder data. Visitor controls ensure visitors are identifiable as visitors so personnel can monitor their activities, and that their access is restricted to just the duration of their legitimate visit. **Definitions** Refer to *Appendix G* for the definition of "visitor."
	9.3.2.b Observe processes when visitors are present in the CDE and interview personnel to verify that visitors are: • Authorized before entering the CDE. • Escorted at all times within the CDE.	
	9.3.2.c Observe the use of visitor badges or other identification to verify that the badge or other identification does not permit unescorted access to the CDE.	
	9.3.2.d Observe visitors in the CDE to verify that: • Visitor badges or other identification are being used for all visitors. • Visitor badges or identification easily distinguish visitors from personnel.	
Customized Approach Objective	**9.3.2.e** Examine visitor badges or other identification and observe evidence in the badging system to verify visitor badges or other identification expires.	
Requirements for visitor access to the CDE are defined and enforced. Visitors cannot exceed any authorized physical access allowed while in the CDE.		

Exhibit 22A-9

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Ensuring that visitor badges are returned or deactivated upon expiry or completion of the visit prevents malicious persons from using a previously authorized pass to gain physical access into the building after the visit has ended.
9.3.3 Visitor badges or identification are surrendered or deactivated before visitors leave the facility or at the date of expiration.	**9.3.3** Observe visitors leaving the facility and interview personnel to verify visitor badges or other identification are surrendered or deactivated before visitors leave the facility or at the date of expiration. upon departure or expiration.	
Customized Approach Objective		
Visitor identification or badges cannot be reused after expiration.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** A visitor log documenting minimum information about the visitor is easy and inexpensive to maintain. It will assist in identifying historical physical access to a building or room and potential access to cardholder data. **Good Practice** When logging the date and time of visit, including both in and out times is considered a best practice, since it provides helpful tracking information and provides assurance that a visitor has left at the end of the day. It is also good to verify that a visitor's ID (driver's license, etc.) matches the name they put on the visitor log.
9.3.4 Visitor logs are used to maintain a physical record of visitor activity both within the facility and within sensitive areas, including: • The visitor's name and the organization represented. • The date and time of the visit. • The name of the personnel authorizing physical access. • Retaining the log for at least three months, unless otherwise restricted by law.	**9.3.4.a** Examine the visitor logs and interview responsible personnel to verify that visitor logs are used to record physical access to both the facility and sensitive areas.	
	9.3.4.b Examine the visitor logs and verify that the logs contain: • The visitor's name and the organization represented. • The personnel authorizing physical access. • Date and time of visit.	
	9.3.4.c Examine visitor log storage locations and interview responsible personnel to verify that the log is retained for at least three months, unless otherwise restricted by law.	
Customized Approach Objective		
Records of visitor access that enable the identification of individuals are maintained.		

Exhibit 22A-9

Requirements and Testing Procedures		Guidance
9.4 Media with cardholder data is securely stored, accessed, distributed, and destroyed.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Controls for physically securing media are intended to prevent unauthorized persons from gaining access to cardholder data on any media. Cardholder data is susceptible to unauthorized viewing, copying, or scanning if it is unprotected while it is on removable or portable media, printed out, or left on someone’s desk.
9.4.1 All media with cardholder data is physically secured.	**9.4.1.** Examine documentation to verify that the procedures defined for protecting cardholder data include controls for physically securing all media.	
Customized Approach Objective		
Media with cardholder data cannot be accessed by unauthorized personnel.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If stored in a non-secured facility, backups containing cardholder data may easily be lost, stolen, or copied for malicious intent. **Good Practice** For secure storage of backup media, a good practice is to store media in an off-site facility, such as an alternate or backup site or commercial storage facility.
9.4.1.1 Offline media backups with cardholder data are stored in a secure location.	**9.4.1.1.a** Examine documentation to verify that procedures are defined for physically securing offline media backups with cardholder data in a secure location.	
	9.4.1.1.b Examine logs or other documentation and interview responsible personnel at the storage location to verify that offline media backups are stored in a secure location.	
Customized Approach Objective		
Offline backups cannot be accessed by unauthorized personnel.		

Exhibit 22A-9

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Conducting regular reviews of the storage facility enables the organization to address identified security issues promptly, minimizing the potential risk. It is important for the entity to be aware of the security of the area where media is being stored.
9.4.1.2 The security of the offline media backup location(s) with cardholder data is reviewed at least once every 12 months.	**9.4.1.2.a** Examine documentation to verify that procedures are defined for reviewing the security of the offline media backup location(s) with cardholder data at least once every 12 months.	
	9.4.1.2.b Examine documented procedures, logs, or other documentation, and interview responsible personnel at the storage location(s) to verify that the storage location's security is reviewed at least once every 12 months.	
Customized Approach Objective		
The security controls protecting offline backups are verified periodically by inspection.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Media not identified as confidential may not be adequately protected or may be lost or stolen. **Good Practice** It is important that media be identified such that its classification status is apparent. This does not mean however that the media needs to have a "confidential" label.
9.4.2 All media with cardholder data is classified in accordance with the sensitivity of the data.	**9.4.2.a** Examine documentation to verify that procedures are defined for classifying media with cardholder data in accordance with the sensitivity of the data.	
	9.4.2.b Examine media logs or other documentation to verify that all media is classified in accordance with the sensitivity of the data.	
Customized Approach Objective		
Media are classified and protected appropriately.		

Exhibit 22A-9

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Media may be lost or stolen if sent via a non-trackable method such as regular postal mail. The use of secure couriers to deliver any media that contains cardholder data allows organizations to use their tracking systems to maintain inventory and location of shipments.
9.4.3 Media with cardholder data sent outside the facility is secured as follows: • Media sent outside the facility is logged. • Media is sent by secured courier or other delivery method that can be accurately tracked. • Offsite tracking logs include details about media location.	**9.4.3.a** Examine documentation to verify that procedures are defined for securing media sent outside the facility in accordance with all elements specified in this requirement.	
	9.4.3.b Interview personnel and examine records to verify that all media sent outside the facility is logged and sent via secured courier or other delivery method that can be tracked.	
	9.4.3.c Examine offsite tracking logs for all media to verify tracking details are documented.	
Customized Approach Objective		
Media is secured and tracked when transported outside the facility.		

Exhibit 22A-9

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Without a firm process for ensuring that all media movements are approved before the media is removed from secure areas, the media would not be tracked or appropriately protected, and its location would be unknown, leading to lost or stolen media.
9.4.4 Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals).	**9.4.4.a** Examine documentation to verify that procedures are defined to ensure that media moved outside the facility is approved by management.	
	9.4.4.b Examine offsite media tracking logs and interview responsible personnel to verify that proper management authorization is obtained for all media moved outside the facility (including media distributed to individuals).	
Customized Approach Objective		
Media cannot leave a facility without the approval of accountable personnel.		
Applicability Notes		
Individuals approving media movements should have the appropriate level of management authority to grant this approval. However, it is not specifically required that such individuals have “manager” as part of their title.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Without careful inventory methods and storage controls, stolen or missing electronic media could go unnoticed for an indefinite amount of time.
9.4.5 Inventory logs of all electronic media with cardholder data are maintained.	**9.4.5.a** Examine documentation to verify that procedures are defined to maintain electronic media inventory logs.	
	9.4.5.b Examine electronic media inventory logs and interview responsible personnel to verify that logs are maintained.	
Customized Approach Objective		
Accurate inventories of stored electronic media are maintained.		

Exhibit 22A-9

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Without careful inventory methods and storage controls, stolen or missing electronic media could go unnoticed for an indefinite amount of time.
9.4.5.1 Inventories of electronic media with cardholder data are conducted at least once every 12 months.	**9.4.5.1.a** Examine documentation to verify that procedures are defined to conduct inventories of electronic media with cardholder data at least once every 12 months.	
	9.4.5.1.b Examine electronic media inventory logs and interview personnel to verify that electronic media inventories are performed at least once every 12 months.	
Customized Approach Objective		
Media inventories are verified periodically.		

Exhibit 22A-9

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If steps are not taken to destroy information contained on hard-copy media before disposal, malicious individuals may retrieve information from the disposed media, leading to a data compromise. For example, malicious individuals may use a technique known as “dumpster diving,” where they search through trashcans and recycle bins looking for hard-copy materials with information they can use to launch an attack. Securing storage containers used for materials that are going to be destroyed prevents sensitive information from being captured while the materials are being collected. **Good Practice** Consider “to-be-shredded” containers with a lock that prevents access to its contents or that physically prevent access to the inside of the container. **Further Information** See *NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization*.
9.4.6 Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows: • Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed. • Materials are stored in secure storage containers prior to destruction.	**9.4.6.a** Examine the media destruction policy to verify that procedures are defined to destroy hard-copy media with cardholder data when no longer needed for business or legal reasons in accordance with all elements specified in this requirement.	
	9.4.6.b Observe processes and interview personnel to verify that hard-copy materials are cross-cut shredded, incinerated, or pulped such that cardholder data cannot be reconstructed.	
	9.4.6.c Observe storage containers used for materials that contain information to be destroyed to verify that the containers are secure.	
Customized Approach Objective		
Cardholder data cannot be recovered from media that has been destroyed or which is pending destruction.		
Applicability Notes		
These requirements for media destruction when that media is no longer needed for business or legal reasons are separate and distinct from PCI DSS Requirement 3.2.1, which is for securely deleting cardholder data when no longer needed per the entity’s cardholder data retention policies.		

Exhibit 22A-9

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If steps are not taken to destroy information contained on electronic media when no longer needed, malicious individuals may retrieve information from the disposed media, leading to a data compromise. For example, malicious individuals may use a technique known as "dumpster diving," where they search through trashcans and recycle bins looking for information they can use to launch an attack. **Good Practice** The deletion function in most operating systems allows deleted data to be recovered, so instead, a dedicated secure deletion function or application should be used to make data unrecoverable. **Examples** Methods for securely destroying electronic media include secure wiping in accordance with industry-accepted standards for secure deletion, degaussing, or physical destruction (such as grinding or shredding hard disks). **Further Information** See *NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization*
9.4.7 Electronic media with cardholder data is destroyed when no longer needed for business or legal reasons via one of the following: • The electronic media is destroyed. • The cardholder data is rendered unrecoverable so that it cannot be reconstructed.	**9.4.7.a** Examine the media destruction policy to verify that procedures are defined to destroy electronic media when no longer needed for business or legal reasons in accordance with all elements specified in this requirement. **9.4.7.b** Observe the media destruction process and interview responsible personnel to verify that electronic media with cardholder data is destroyed via one of the methods specified in this requirement.	
Customized Approach Objective		
Cardholder data cannot be recovered from media that has been erased or destroyed.		
Applicability Notes		
These requirements for media destruction when that media is no longer needed for business or legal reasons are separate and distinct from PCI DSS Requirement 3.2.1, which is for securely deleting cardholder data when no longer needed per the entity's cardholder data retention policies.		

Exhibit 22A-9

Requirements and Testing Procedures		Guidance
9.5 Point-of-interaction (POI) devices are protected from tampering and unauthorized substitution.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Criminals attempt to steal payment card data by stealing and/or manipulating card-reading devices and terminals. Criminals will try to steal devices so they can learn how to break into them, and they often try to replace legitimate devices with fraudulent devices that send them payment card data every time a card is entered. They will also try to add “skimming” components to the outside of devices, which are designed to capture payment card data before it enters the device—for example, by attaching an additional card reader on top of the legitimate card reader so that the payment card data is captured twice: once by the criminal’s component and then by the device’s legitimate component. In this way, transactions may still be completed without interruption while the criminal is “skimming” the payment card data during the process.
9.5.1 POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: • Maintaining a list of POI devices. • Periodically inspecting POI devices to look for tampering or unauthorized substitution. • Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	**9.5.1** Examine documented policies and procedures to verify that processes are defined that include all elements specified in this requirement.	
Customized Approach Objective		
The entity has defined procedures to protect and manage point-of-interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.		

Exhibit 22A-9

Requirements and Testing Procedures		Guidance
Applicability Notes		*(continued on next page)*
These requirements apply to deployed POI devices used in card-present transactions (that is, a payment card form factor such as a card that is swiped, tapped, or dipped). These requirements do not apply to: • Components used only for manual PAN key entry. • Commercial off-the-shelf (COTS) devices (for example, smartphones or tablets), which are mobile merchant-owned devices designed for mass-market distribution.		**Good Practice** Entities may consider implementing protection from tampering and unauthorized substitution for: • Components used only for manual PAN key entry. • Commercial off-the-shelf (COTS) devices (for example, smartphones or tablets), which are mobile merchant-owned devices designed for mass-market distribution. **Further Information** Additional best practices on skimming prevention are available on the PCI SSC website.
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
9.5.1.1 An up-to-date list of POI devices is maintained, including: • Make and model of the device. • Location of device. • Device serial number or other methods of unique identification.	**9.5.1.1.a** Examine the list of POI devices to verify it includes all elements specified in this requirement. **9.5.1.1.b** Observe POI devices and device locations and compare to devices in the list to verify that the list is accurate and up to date.	Keeping an up-to-date list of POI devices helps an organization track where devices are supposed to be and quickly identify if a device is missing or lost. *(continued on next page)*

Exhibit 22A-9

Requirements and Testing Procedures		Guidance
Customized Approach Objective The identity and location of POI devices is recorded and known at all times.	**9.5.1.1.c** Interview personnel to verify the list of POI devices is updated when devices are added, relocated, decommissioned, etc.	**Good Practice** The method for maintaining a list of devices may be automated (for example, a device-management system) or manual (for example, documented in electronic or paper records). For on-the-road devices, the location may include the name of the personnel to whom the device is assigned. **Examples** Methods to maintain device locations include identifying the address of the site or facility where the device is located.

Exhibit 22A-9

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Regular inspections of devices will help organizations detect tampering more quickly via external evidence—for example, the addition of a card skimmer—or replacement of a device, thereby minimizing the potential impact of using fraudulent devices. **Good Practice** Methods for periodic inspection include checking the serial number or other device characteristics and comparing the information to the list of POI devices to verify the device has not been swapped with a fraudulent device. *(continued on next page)*
9.5.1.2 POI device surfaces are periodically inspected to detect tampering and unauthorized substitution.	**9.5.1.2.a** Examine documented procedures to verify processes are defined for periodic inspections of POI device surfaces to detect tampering and unauthorized substitution.	
	9.5.1.2.b Interview responsible personnel and observe inspection processes to verify: • Personnel are aware of procedures for inspecting devices. • All devices are periodically inspected for evidence of tampering and unauthorized substitution.	
Customized Approach Objective		
Point of interaction devices cannot be tampered with, substituted without authorization, or have skimming attachments installed without timely detection.		

Exhibit 22A-9

Requirements and Testing Procedures		Guidance
9.5.1.2 *(continued)*		**Examples** The type of inspection will depend on the device. For instance, photographs of devices known to be secure can be used to compare a device's current appearance with its original appearance to see whether it has changed. Another option may be to use a secure marker pen, such as a UV light marker, to mark device surfaces and device openings so any tampering or replacement will be apparent. Criminals will often replace the outer casing of a device to hide their tampering, and these methods may help to detect such activities. Device vendors may also provide security guidance and "how to" guides to help determine whether the device has been subject to tampering. Signs that a device might have been tampered with or substituted include: • Unexpected attachments or cables plugged into the device. • Missing or changed security labels. • Broken or differently colored casing. • Changes to the serial number or other external markings.

Exhibit 22A-9

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Entities are best placed to determine the frequency of POI device inspections based on the environment in which the device operates. **Good Practice** The frequency of inspections will depend on factors such as the location of a device and whether the device is attended or unattended. For example, devices left in public areas without supervision by the organization's personnel might have more frequent inspections than devices kept in secure areas or supervised when accessible to the public. In addition, many POI vendors include guidance in their user documentation about how often POI devices should be checked, and for what – entities should consult their vendors' documentation and incorporate those recommendations into their periodic inspections.
9.5.1.2.1 The frequency of periodic POI device inspections and the type of inspections performed is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.	**9.5.1.2.1.a** Examine the entity's targeted risk analysis for the frequency of periodic POI device inspections and type of inspections performed to verify the risk analysis was performed in accordance with all elements specified in Requirement 12.3.1.	
	9.5.1.2.1.b Examine documented results of periodic device inspections and interview personnel to verify that the frequency and type of POI device inspections performed match what is defined in the entity's targeted risk analysis conducted for this requirement.	
Customized Approach Objective		
POI devices are inspected at a frequency that addresses the entity's risk.		
Applicability Notes		
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.		

Exhibit 22A-9

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Criminals will often pose as authorized maintenance personnel to gain access to POI devices. **Good Practice** Personnel training should include being alert to and questioning anyone who shows up to do POI maintenance to ensure they are authorized and have a valid work order, including any agents, maintenance or repair personnel, technicians, service providers, or other third parties. All third parties requesting access to devices should always be verified before being provided access—for example, by checking with management or phoning the POI maintenance company, such as the vendor or acquirer, for verification. Many criminals will try to fool personnel by dressing for the part (for example, carrying toolboxes and dressed in work apparel), and could also be knowledgeable about locations of devices, so personnel should be trained to always follow procedures. Another trick that criminals use is to send a “new” POI device with instructions for swapping it with a legitimate device and “returning” the legitimate device. The criminals may even provide return postage to their specified address. Therefore, personnel should always verify with their manager or supplier that the device is legitimate and came from a trusted source before installing it or using it for business. *(continued on next page)*
9.5.1.3 Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes: • Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices. • Procedures to ensure devices are not installed, replaced, or returned without verification. • Being aware of suspicious behavior around devices. • Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.	**9.5.1.3.a** Review training materials for personnel in POI environments to verify they include all elements specified in this requirement.	
	9.5.1.3.b Interview personnel in POI environments to verify they have received training and know the procedures for all elements specified in this requirement**.**	
Customized Approach Objective		
Personnel are knowledgeable about the types of attacks against POI devices, the entity’s technical and procedural countermeasures, and can access assistance and guidance when required.		

Exhibit 22A-9

Requirements and Testing Procedures		Guidance
9.5.1.3 *(continued)*		**Examples** Suspicious behavior that personnel should be aware of includes attempts by unknown persons to unplug or open devices. Ensuring personnel are aware of mechanisms for reporting suspicious behavior and who to report such behavior to—for example, a manager or security officer—will help reduce the likelihood and potential impact of a device being tampered with or substituted.

Exhibit 22A-10

Regularly Monitor and Test Networks

Requirement 10: Log and Monitor All Access to System Components and Cardholder Data

Sections

10.1 Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and understood.

10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.

10.3 Audit logs are protected from destruction and unauthorized modifications.

10.4 Audit logs are reviewed to identify anomalies or suspicious activity.

10.5 Audit log history is retained and available for analysis.

10.6 Time-synchronization mechanisms support consistent time settings across all systems.

10.7 Failures of critical security control systems are detected, reported, and responded to promptly.

Overview

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs on all system components and in the cardholder data environment (CDE) allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is difficult, if not impossible, without system activity logs.

This requirement applies to user activities, including those by employees, contractors, consultants, and internal and external vendors, and other third parties (for example, those providing support or maintenance services).

These requirements do not apply to user activity of consumers (cardholders).

Refer to *Appendix G* for definitions of PCI DSS terms.

Exhibit 22A-10

Requirements and Testing Procedures		Guidance
10.1 Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and understood.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Requirement 10.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 10. While it is important to define the specific policies or procedures called out in Requirement 10, it is equally important to ensure they are properly documented, maintained, and disseminated. **Good Practice** It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle. **Definitions** Security policies define the entity's security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives.
10.1.1 All security policies and operational procedures that are identified in Requirement 10 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	**10.1.1** Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 10 are managed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Expectations, controls, and oversight for meeting activities within Requirement 10 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.		

Exhibit 22A-10

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and critical activities may not occur. **Good Practice** Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities. **Examples** A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).
10.1.2 Roles and responsibilities for performing activities in Requirement 10 are documented, assigned, and understood.	**10.1.2.a** Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 10 are documented and assigned.	
	10.1.2.b Interview personnel with responsibility for performing activities in Requirement 10 to verify that roles and responsibilities are assigned as defined and are understood.	
Customized Approach Objective		
Day-to-day responsibilities for performing all the activities in Requirement 10 are allocated. Personnel are accountable for successful, continuous operation of these requirements.		

Exhibit 22A-10

Requirements and Testing Procedures		Guidance
10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Audit logs must exist for all system components. Audit logs send alerts the system administrator, provides data to other monitoring mechanisms, such as intrusion-detection systems (IDS) and security information and event monitoring systems (SIEM) tools, and provide a history trail for post-incident investigation. Logging and analyzing security-relevant events enable an organization to identify and trace potentially malicious activities. **Good Practice** When an entity considers which information to record in their logs, it is important to remember that information stored in audit logs is sensitive and should be protected per requirements in this standard. Care should be taken to only store essential information in the audit logs to minimize risk.
10.2.1 Audit logs are enabled and active for all system components and cardholder data.	**10.2.1** Interview the system administrator and examine system configurations to verify that audit logs are enabled and active for all system components.	
Customized Approach Objective		
Records of all activities affecting system components and cardholder data are captured.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** It is critical to have a process or system that links user access to system components accessed. Malicious individuals could obtain knowledge of a user account with access to systems in the CDE, or they could create a new, unauthorized account to access cardholder data. **Good Practice** A record of all individual access to cardholder data can identify which accounts may have been compromised or misused.
10.2.1.1 Audit logs capture all individual user access to cardholder data.	**10.2.1.1** Examine audit log configurations and log data to verify that all individual user access to cardholder data is logged.	
Customized Approach Objective		
Records of all individual user access to cardholder data are captured.		

Exhibit 22A-10

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Accounts with increased access privileges, such as the “administrator” or “root” account, have the potential to significantly impact the security or operational functionality of a system. Without a log of the activities performed, an organization is cannot trace any issues resulting from an administrative mistake or misuse of privilege back to the specific action and account. **Definitions** The functions or activities considered to be administrative are beyond those performed by regular users as part of routine business functions. Refer to *Appendix G* for the definition of “administrative access.”
10.2.1.2 Audit logs capture all actions taken by any individual with administrative access, including any interactive use of application or system accounts.	**10.2.1.2** Examine audit log configurations and log data to verify that all actions taken by any individual with administrative access, including any interactive use of application or system accounts, are logged.	
Customized Approach Objective		
Records of all actions performed by individuals with elevated privileges are captured.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Malicious users often attempt to alter audit logs to hide their actions. A record of access allows an organization to trace any inconsistencies or potential tampering of the logs to an individual account. Having logs identify changes, additions, and deletions to the audit logs can help retrace steps made by unauthorized personnel.
10.2.1.3 Audit logs capture all access to audit logs.	**10.2.1.3** Examine audit log configurations and log data to verify that access to all audit logs is captured.	
Customized Approach Objective		
Records of all access to audit logs are captured.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Malicious individuals will often perform multiple access attempts on targeted systems. Multiple
10.2.1.4 Audit logs capture all invalid logical access attempts.		

Exhibit 22A-10

Requirements and Testing Procedures		Guidance
Customized Approach Objective Records of all invalid access attempts are captured.	**10.2.1.4** Examine audit log configurations and log data to verify that invalid logical access attempts are captured.	invalid login attempts may be an indication of an unauthorized user's attempts to "brute force" or guess a password.

Exhibit 22A-10

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
10.2.1.5 Audit logs capture all changes to identification and authentication credentials including, but not limited to: • Creation of new accounts. • Elevation of privileges. • All changes, additions, or deletions to accounts with administrative access.	**10.2.1.5** Examine audit log configurations and log data to verify that changes to identification and authentication credentials are captured in accordance with all elements specified in this requirement.	Logging changes to authentication credentials (including elevation of privileges, additions, and deletions of accounts with administrative access) provides residual evidence of activities. Malicious users may attempt to manipulate authentication credentials to bypass them or impersonate a valid account.
Customized Approach Objective		
Records of all changes to identification and authentication credentials are captured.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
10.2.1.6 Audit logs capture the following: • All initialization of new audit logs, and • All starting, stopping, or pausing of the existing audit logs.	**10.2.1.6** Examine audit log configurations and log data to verify that all elements specified in this requirement are captured.	Turning off or pausing audit logs before performing illicit activities is common practice for malicious users who want to avoid detection. Initialization of audit logs could indicate that that a user disabled the log function to hide their actions.
Customized Approach Objective		
Records of all changes to audit log activity status are captured.		

Exhibit 22A-10

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Malicious software, such as malware, often creates or replaces system-level objects on the target system to control a particular function or operation on that system. By logging when system-level objects are created or deleted, it will be easier to determine whether such modifications were authorized.
10.2.1.7 Audit logs capture all creation and deletion of system-level objects.	**10.2.1.7** Examine audit log configurations and log data to verify that creation and deletion of system level objects is captured.	
Customized Approach Objective		
Records of alterations that indicate a system has been modified from its intended functionality are captured.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** By recording these details for the auditable events at 10.2.1.1 through 10.2.1.7, a potential compromise can be quickly identified, with sufficient detail to facilitate following up on suspicious activities.
10.2.2 Audit logs record the following details for each auditable event: • User identification. • Type of event. • Date and time. • Success and failure indication. • Origination of event. • Identity or name of affected data, system component, resource, or service (for example, name and protocol).	**10.2.2** Interview personnel and examine audit log configurations and log data to verify that all elements specified in this requirement are included in log entries for each auditable event (from 10.2.1.1 through 10.2.1.7).	
Customized Approach Objective		
Sufficient data to be able to identify successful and failed attempts and who, what, when, where, and how for each event listed in requirement 10.2.1 are captured.		

Exhibit 22A-10

Requirements and Testing Procedures		Guidance
10.3 Audit logs are protected from destruction and unauthorized modifications.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Audit log files contain sensitive information, and read access to the log files must be limited only to those with a valid business need. This access includes audit log files on the originating systems as well as anywhere else they are stored. **Good Practice** Adequate protection of the audit logs includes strong access control that limits access to logs based on "need to know" only and the use of physical or network segregation to make the logs harder to find and modify.
10.3.1 Read access to audit logs files is limited to those with a job-related need.	**10.3.1** Interview system administrators and examine system configurations and privileges to verify that only individuals with a job-related need have read access to audit log files.	
Customized Approach Objective		
Stored activity records cannot be accessed by unauthorized personnel.		

Exhibit 22A-10

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Often a malicious individual who has entered the network will try to edit the audit logs to hide their activity. Without adequate protection of audit logs, their completeness, accuracy, and integrity cannot be guaranteed, and the audit logs can be rendered useless as an investigation tool after a compromise. Therefore, audit logs should be protected on the originating systems as well as anywhere else they are stored. **Good Practice** Entities should attempt to prevent logs from being exposed in public-accessible locations.
10.3.2 Audit log files are protected to prevent modifications by individuals.	**10.3.2** Examine system configurations and privileges and interview system administrators to verify that current audit log files are protected from modifications by individuals via access control mechanisms, physical segregation, and/or network segregation.	
Customized Approach Objective		
Stored activity records cannot be modified by personnel.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Promptly backing up the logs to a centralized log server or media that is difficult to alter keeps the logs protected, even if the system generating the logs becomes compromised. Writing logs from external-facing technologies such as wireless, network security controls, DNS, and mail servers, reduces the risk of those logs being lost or altered. **Good Practice** Each entity determines the best way to back up log files, whether via one or more centralized log servers or other secure media. Logs may be written directly, offloaded, or copied from external systems to the secure internal system or media.
10.3.3 Audit log files, including those for external-facing technologies, are promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify.	**10.3.3** Examine backup configurations or log files to verify that current audit log files, including those for external-facing technologies, are promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify.	
Customized Approach Objective		
Stored activity records are secured and preserved in a central location to prevent unauthorized modification.		

Exhibit 22A-10

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** File integrity monitoring or change-detection systems check for changes to critical files and notify when such changes are identified. For file integrity monitoring purposes, an entity usually monitors files that do not regularly change, but when changed, indicate a possible compromise. **Good Practice** Software used to monitor changes to audit logs should be configured to provide alerts when existing log data or files are changed or deleted. However, new log data being added to an audit log should not generate an alert.
10.3.4 File integrity monitoring or change-detection mechanisms is used on audit logs to ensure that existing log data cannot be changed without generating alerts.	**10.3.4** Examine system settings, monitored files, and results from monitoring activities to verify the use of file integrity monitoring or change-detection software on audit logs.	
Customized Approach Objective		
Stored activity records cannot be modified without an alert being generated.		

Exhibit 22A-10

Requirements and Testing Procedures		Guidance
10.4 Audit logs are reviewed to identify anomalies or suspicious activity.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Many breaches occur months before being detected. Regular log reviews mean incidents can be quickly identified and proactively addressed. **Good Practice** Checking logs daily (7 days a week, 365 days a year, including holidays) minimizes the amount of time and exposure of a potential breach. Log harvesting, parsing, and alerting tools, centralized log management systems, event log analyzers, and security information and event management (SIEM) solutions are examples of automated tools that can be used to meet this requirement. Daily review of security events—for example, notifications or alerts that identify suspicious or anomalous activities—as well as logs from critical system components, and logs from systems that perform security functions, such as firewalls, IDS/IPS, file integrity monitoring (FIM) systems, etc., is necessary to identify potential issues. The determination of "security event" will vary for each organization and may include consideration for the type of technology, location, and function of the device. Organizations may also wish to maintain a baseline of "normal" traffic to help identify anomalous behavior. An entity that uses third-party service providers to perform log review services is responsible to provide context about the entity's environment to the service providers, so it understands the entity's environment, has a baseline of "normal" traffic for the entity, and can detect potential security issues and provide accurate exceptions and anomaly notifications.
10.4.1 The following audit logs are reviewed at least once daily: • All security events. • Logs of all system components that store, process, or transmit CHD and/or SAD. • Logs of all critical system components. • Logs of all servers and system components that perform security functions (for example, network security controls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers).	**10.4.1.a** Examine security policies and procedures to verify that processes are defined for reviewing all elements specified in this requirement at least once daily. **10.4.1.b** Observe processes and interview personnel to verify that all elements specified in this requirement are reviewed at least once daily	
Customized Approach Objective		
Potentially suspicious or anomalous activities are quickly identified to minimize impact.		

Exhibit 22A-10

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Manual log reviews are difficult to perform, even for one or two systems, due to the amount of log data that is generated. However, using log harvesting, parsing, and alerting tools, centralized log management systems, event log analyzers, and security information and event management (SIEM) solutions can help facilitate the process by identifying log events that need to be reviewed. **Good Practice** Establishing a baseline of normal audit activity patterns is critical to the effectiveness of an automated log review mechanism. The analysis of new audit activity against the established baseline can significantly improve the identification of suspicious or anomalous activities. The entity should keep logging tools aligned with any changes in their environment by periodically reviewing tool settings and updating settings to reflect any changes. **Further Information** Refer to the Information Supplement: *Effective Daily Log Monitoring* for additional guidance.
10.4.1.1 Automated mechanisms are used to perform audit log reviews.	**10.4.1.1** Examine log review mechanisms and interview personnel to verify that automated mechanisms are used to perform log reviews.	
Customized Approach Objective		
Potentially suspicious or anomalous activities are identified via a repeatable and consistent mechanism.		
Applicability Notes		
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.		

Exhibit 22A-10

<table>
<tr><th colspan="2">Requirements and Testing Procedures</th><th>Guidance</th></tr>
<tr><td><b>Defined Approach Requirements</b></td><td><b>Defined Approach Testing Procedures</b></td><td rowspan="7"><b>Purpose</b>
Periodic review of logs for all other system components (not specified in Requirement 10.4.1) helps to identify indications of potential issues or attempts to access critical systems via less-critical systems.</td></tr>
<tr><td rowspan="2"><b>10.4.2</b> Logs of all other system components (those not specified in Requirement 10.4.1) are reviewed periodically.</td><td><b>10.4.2.a</b> Examine security policies and procedures to verify that processes are defined for reviewing logs of all other system components periodically.</td></tr>
<tr><td rowspan="5"><b>10.4.2.b</b> Examine documented results of log reviews and interview personnel to verify that log reviews are performed periodically.</td></tr>
<tr><td><b>Customized Approach Objective</b></td></tr>
<tr><td>Potentially suspicious or anomalous activities for other system components (not included in 10.4.1) are reviewed in accordance with the entity's identified risk.</td></tr>
<tr><td><b>Applicability Notes</b></td></tr>
<tr><td>This requirement is applicable to all other in-scope system components not included in Requirement 10.4.1.</td></tr>
</table>

Exhibit 22A-10

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Entities can determine the optimum period to review these logs based on criteria such as the complexity of each entity's environment, the number of types of systems that are required to be evaluated, and the functions of such systems.
10.4.2.1 The frequency of periodic log reviews for all other system components (not defined in Requirement 10.4.1) is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1	**10.4.2.1.a** Examine the entity's targeted risk analysis for the frequency of periodic log reviews for all other system components (not defined in Requirement 10.4.1) to verify the risk analysis was performed in accordance with all elements specified at Requirement 12.3.1.	
Customized Approach Objective Log reviews for lower-risk system components are performed at a frequency that addresses the entity's risk. **Applicability Notes** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	**10.4.2.1.b** Examine documented results of periodic log reviews of all other system components (not defined in Requirement 10.4.1) and interview personnel to verify log reviews are performed at the frequency specified in the entity's targeted risk analysis performed for this requirement.	

Exhibit 22A-10

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If exceptions and anomalies identified during the log-review process are not investigated, the entity may be unaware of unauthorized and potentially malicious activities occurring within their network. **Good Practice** Entities should consider how to address the following when developing their processes for defining and managing exceptions and anomalies: • How log review activities are recorded, • How to rank and prioritize exceptions and anomalies, • What procedures should be in place to report and escalate exceptions and anomalies, and • Who is responsible for investigating and for any remediation tasks.
10.4.3 Exceptions and anomalies identified during the review process are addressed.	**10.4.3.a** Examine security policies and procedures to verify that processes are defined for addressing exceptions and anomalies identified during the review process.	
	10.4.3.b Observe processes and interview personnel to verify that, when exceptions and anomalies are identified, they are addressed.	
Customized Approach Objective		
Suspicious or anomalous activities are addressed.		

Exhibit 22A-10

Requirements and Testing Procedures		Guidance
10.5 Audit log history is retained and available for analysis.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Retaining historical audit logs for at least 12 months is necessary because compromises often go unnoticed for significant lengths of time. Having centrally stored log history allows investigators to better determine the length of time a potential breach was occurring, and the possible system(s) impacted. By having three months of logs immediately available, an entity can quickly identify and minimize impact of a data breach. **Examples** Methods that allow logs to be immediately available include storing logs online, archiving logs, or restoring logs quickly from backups.
10.5.1 Retain audit log history for at least 12 months, with at least the most recent three months immediately available for analysis.	**10.5.1.a** Examine documentation to verify that the following is defined: • Audit log retention policies. • Procedures for retaining audit log history for at least 12 months, with at least the most recent three months immediately available online.	
	10.5.1.b Examine configurations of audit log history, interview personnel and examine audit logs to verify that audit logs history is retained for at least 12 months.	
Customized Approach Objective	**10.5.1.c** Interview personnel and observe processes to verify that at least the most recent three months' audit log history is immediately available for analysis.	
Historical records of activity are available immediately to support incident response and are retained for at least 12 months.		

Exhibit 22A-10

Requirements and Testing Procedures		Guidance
10.6 Time-synchronization mechanisms support consistent time settings across all systems.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Time synchronization technology is used to synchronize clocks on multiple systems. When clocks are not properly synchronized, it can be difficult, if not impossible, to compare log files from different systems and establish an exact sequence of events, which is crucial for forensic analysis following a breach. For post-incident forensics teams, the accuracy and consistency of time across all systems and the time of each activity are critical in determining how the systems were compromised. **Examples** Network Time Protocol (NTP) is one example of time-synchronization technology.
10.6.1 System clocks and time are synchronized using time-synchronization technology.	**10.6.1** Examine system configuration settings to verify that time-synchronization technology is implemented and kept current.	
Customized Approach Objective		
Common time is established across all systems.		
Applicability Notes		
Keeping time-synchronization technology current includes managing vulnerabilities and patching the technology according to PCI DSS Requirements 6.3.1 and 6.3.3.		

Exhibit 22A-10

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Using reputable time servers is a critical component of the time synchronization process. Accepting time updates from specific, industry-accepted external sources helps prevent a malicious individual from changing time settings on systems. **Good Practice** Another option to prevent unauthorized use of internal time servers is to encrypt updates with a symmetric key and create access control lists that specify the IP addresses of client machines that will be provided with the time updates.
10.6.2 Systems are configured to the correct and consistent time as follows: • One or more designated time servers are in use. • Only the designated central time server(s) receives time from external sources. • Time received from external sources is based on International Atomic Time or Coordinated Universal Time (UTC). • The designated time server(s) accept time updates only from specific industry-accepted external sources. • Where there is more than one designated time server, the time servers peer with one another to keep accurate time. • Internal systems receive time information only from designated central time server(s).	**10.6.2** Examine system configuration settings for acquiring, distributing, and storing the correct time to verify the settings are configured in accordance with all elements specified in this requirement.	
Customized Approach Objective		
The time on all systems is accurate and consistent.		

Exhibit 22A-10

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Attackers will try to change time configurations to hide their activity. Therefore, restricting the ability to change or modify time synchronization configurations or the system time to administrators will lessen the probability of an attacker successfully changing time configurations.
10.6.3 Time synchronization settings and data are protected as follows: • Access to time data is restricted to only personnel with a business need. • Any changes to time settings on critical systems are logged, monitored, and reviewed.	**10.6.3.a** Examine system configurations and time-synchronization settings to verify that access to time data is restricted to only personnel with a business need.	
	10.6.3.b Examine system configurations and time synchronization settings and logs and observe processes to verify that any changes to time settings on critical systems are logged, monitored, and reviewed.	
Customized Approach Objective		
System time settings cannot be modified by unauthorized personnel.		

Exhibit 22A-10

Requirements and Testing Procedures		Guidance
10.7 Failures of critical security control systems are detected, reported, and responded to promptly.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Without formal processes to detect and alert when critical security controls fail, failures may go undetected for extended periods and provide attackers ample time to compromise system components and steal account data from the CDE. **Good Practice** The specific types of failures may vary, depending on the function of the device system component and technology in use. Typical failures include a system ceasing to perform its security function or not functioning in its intended manner, such as a firewall erasing all its rules or going offline.
10.7.1 ***Additional requirement for service providers only:*** Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls. • IDS/IPS. • FIM. • Anti-malware solutions. • Physical access controls. • Logical access controls. • Audit logging mechanisms. • Segmentation controls (if used).	**10.7.1.a** ***Additional testing procedure for service provider assessments only:*** Examine documentation to verify that processes are defined for the prompt detection and addressing of failures of critical security control systems, including but not limited to failure of all elements specified in this requirement.	
	10.7.1.b ***Additional testing procedure for service provider assessments only:*** Observe detection and alerting processes and interview personnel to verify that failures of critical security control systems are detected and reported, and that failure of a critical security control results in the generation of an alert.	
Customized Approach Objective		
Failures in critical security control systems are promptly identified and addressed.		
Applicability Notes		
This requirement applies only when the entity being assessed is a service provider. *This requirement will be superseded by Requirement 10.7.2 as of 31 March 2025.*		

Exhibit 22A-10

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Without formal processes to detect and alert when critical security controls fail, failures may go undetected for extended periods and provide attackers ample time to compromise system components and steal account data from the CDE. **Good Practice** The specific types of failures may vary, depending on the function of the device system component and technology in use. However, typical failures include a system no longer performing its security function or not functioning in its intended manner—for example, a firewall erasing its rules or going offline.
10.7.2 Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls. • IDS/IPS. • Change-detection mechanisms. • Anti-malware solutions. • Physical access controls. • Logical access controls. • Audit logging mechanisms. • Segmentation controls (if used). • Audit log review mechanisms. • Automated security testing tools (if used).	**10.7.2.a** Examine documentation to verify that processes are defined for the prompt detection and addressing of failures of critical security control systems, including but not limited to failure of all elements specified in this requirement.	
	10.7.2.b Observe detection and alerting processes and interview personnel to verify that failures of critical security control systems are detected and reported, and that failure of a critical security control results in the generation of an alert.	
Customized Approach Objective		
Failures in critical security control systems are promptly identified and addressed.		
Applicability Notes		
This requirement applies to all entities, including service providers, and will supersede Requirement 10.7.1 as of 31 March 2025. It includes two additional critical security control systems not in Requirement 10.7.1. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

Exhibit 22A-10

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If alerts from failures of critical security control systems are not responded to quickly and effectively, attackers may use this time to insert malicious software, gain control of a system, or steal data from the entity's environment. **Good Practice** Documented evidence (for example, records within a problem management system) should provide support that processes and procedures are in place to respond to security failures. In addition, personnel should be aware of their responsibilities in the event of a failure. Actions and responses to the failure should be captured in the documented evidence.
10.7.3 Failures of any critical security control systems are responded to promptly, including but not limited to: • Restoring security functions. • Identifying and documenting the duration (date and time from start to end) of the security failure. • Identifying and documenting the cause(s) of failure and documenting required remediation. • Identifying and addressing any security issues that arose during the failure. • Determining whether further actions are required as a result of the security failure. • Implementing controls to prevent the cause of failure from reoccurring. • Resuming monitoring of security controls.	**10.7.3.a** Examine documentation and interview personnel to verify that processes are defined and implemented to respond to a failure of any critical security control system and include at least all elements specified in this requirement.	
	10.7.3.b Examine records to verify that failures of critical security control systems are documented to include: • Identification of cause(s) of the failure. • Duration (date and time start and end) of the security failure. • Details of the remediation required to address the root cause.	
Customized Approach Objective		
Failures of critical security control systems are analyzed, contained, and resolved, and security controls restored to minimize impact. Resulting security issues are addressed, and measures taken to prevent reoccurrence. *(continued on next page)*		

Exhibit 22A-10

Requirements and Testing Procedures		Guidance
Applicability Notes This requirement applies only when the entity being assessed is a service provider until 31 March 2025, after which this requirement will apply to all entities. *This is a current v3.2.1 requirement that applies to service providers only. However, this requirement is a best practice for all other entities until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

Exhibit 22A-11

Requirement 11:Test Security of Systems and Networks Regularly

Sections

11.1 Processes and mechanisms for regularly testing security of systems and networks are defined and understood.

11.2 Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.

11.3 External and internal vulnerabilities are regularly identified, prioritized, and addressed.

11.4 External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.

11.5 Network intrusions and unexpected file changes are detected and responded to.

11.6 Unauthorized changes on payment pages are detected and responded to.

Overview

Vulnerabilities are being discovered continually by malicious individuals and researchers, as well as being introduced by new software. System components, processes, and bespoke and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

Refer to *Appendix G* for definitions of PCI DSS terms.

Exhibit 22A-11

Requirements and Testing Procedures		Guidance
11.1 Processes and mechanisms for regularly testing security of systems and networks are defined and understood.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Requirement 11.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 11. While it is important to define the specific policies or procedures called out in Requirement 11, it is equally important to ensure they are properly documented, maintained, and disseminated. **Good Practice** It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle. **Definitions** Security policies define the entity's security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives.
11.1.1 All security policies and operational procedures that are identified in Requirement 11 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	**11.1.1** Examine documentation and interview personnel to verify that security policies and operational procedures are managed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Expectations, controls, and oversight for meeting activities within Requirement 11 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.		

Exhibit 22A-11

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and critical activities may not occur. **Good Practice** Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities. **Examples** A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).
11.1.2 Roles and responsibilities for performing activities in Requirement 11 are documented, assigned, and understood.	**11.1.2.a** Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 11 are documented and assigned.	
	11.1.2.b Interview personnel with responsibility for performing activities in Requirement 11 to verify that roles and responsibilities are assigned as documented and are understood.	
Customized Approach Objective		
Day-to-day responsibilities for performing all the activities in Requirement 11 are allocated. Personnel are accountable for successful, continuous operation of these requirements.		

Exhibit 22A-11

Requirements and Testing Procedures		Guidance
11.2 Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Implementation and/or exploitation of wireless technology within a network are common paths for malicious users to gain unauthorized access to the network and cardholder data. Unauthorized wireless devices could be hidden within or attached to a computer or other system component. These devices could also be attached directly to a network port, to a network device such as a switch or router, or inserted as a wireless interface card inside a system component. Even if a company has a policy prohibiting the use of wireless technologies, an unauthorized wireless device or network could be installed without the company's knowledge, allowing an attacker to enter the network easily and "invisibly." Detecting and removing such unauthorized access points reduces the duration and likelihood of such devices being leveraged for an attack. *(continued on next page)*
11.2.1 Authorized and unauthorized wireless access points are managed as follows: • The presence of wireless (Wi-Fi) access points is tested for, • All authorized and unauthorized wireless access points are detected and identified, • Testing, detection, and identification occurs at least once every three months. • If automated monitoring is used, personnel are notified via generated alerts.	**11.2.1.a** Examine policies and procedures to verify processes are defined for managing both authorized and unauthorized wireless access points with all elements specified in this requirement.	
	11.2.1.b Examine the methodology(ies) in use and the resulting documentation, and interview personnel to verify processes are defined to detect and identify both authorized and unauthorized wireless access points in accordance with all elements specified in this requirement.	
	11.2.1.c Examine wireless assessment results and interview personnel to verify that wireless assessments were conducted in accordance with all elements specified in this requirement.	
Customized Approach Objective	**11.2.1.d** If automated monitoring is used, examine configuration settings to verify the configuration will generate alerts to notify personnel.	
Unauthorized wireless access points are identified and addressed periodically.		

Exhibit 22A-11

Requirements and Testing Procedures		Guidance
Applicability Notes The requirement applies even when a policy exists that prohibits the use of wireless technology. Methods used to meet this requirement must be sufficient to detect and identify both authorized and unauthorized devices, including unauthorized devices attached to devices that themselves are authorized.		**Good Practice** The size and complexity of an environment will dictate the appropriate tools and processes to be used to provide sufficient assurance that a rogue wireless access point has not been installed in the environment. For example, performing a detailed physical inspection of a single stand-alone retail kiosk in a shopping mall, where all communication components are contained within tamper-resistant and tamper-evident casings, may be sufficient to provide assurance that a rogue wireless access point has not been attached or installed. However, in an environment with multiple nodes (such as in a large retail store, call center, server room or data center), detailed physical inspection can be difficult. In this case, multiple methods may be combined, such as performing physical system inspections in conjunction with the results of a wireless analyzer. **Definitions** This is also referred to as rogue access point detection. **Examples** Methods that may be used include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. NAC and wireless IDS/IPS are examples of automated monitoring tools.

Exhibit 22A-11

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** An inventory of authorized wireless access points can help administrators quickly respond when unauthorized wireless access points are detected. This helps to proactively minimize the exposure of CDE to malicious individuals. **Good Practice** If using a wireless scanner, it is equally important to have a defined list of known access points which, while not attached to the company's network, will usually be detected during a scan. These non-company devices are often found in multi-tenant buildings or businesses located near one another. However, it is important to verify that these devices are not connected to the entity's network port or through another network-connected device and given an SSID resembling a nearby business. Scan results should note such devices and how it was determined that these devices could be "ignored." In addition, detection of any unauthorized wireless access points that are determined to be a threat to the CDE should be managed following the entity's incident response plan per Requirement 12.10.1.
11.2.2 An inventory of authorized wireless access points is maintained, including a documented business justification.	**11.2.2** Examine documentation to verify that an inventory of authorized wireless access points is maintained, and a business justification is documented for all authorized wireless access points.	
Customized Approach Objective		
Unauthorized wireless access points are not mistaken for authorized wireless access points.		

Exhibit 22A-11

Requirements and Testing Procedures		Guidance
11.3 External and internal vulnerabilities are regularly identified, prioritized, and addressed.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Identifying and addressing vulnerabilities promptly reduces the likelihood of a vulnerability being exploited and the potential compromise of a system component or cardholder data. Vulnerability scans conducted at least every three months provide this detection and identification. **Good Practice** Vulnerabilities posing the greatest risk to the environment (for example, ranked high or critical per Requirement 6.3.1) should be resolved with the highest priority. Vulnerabilities identified during internal vulnerability scans should be part of a vulnerability management process that includes multiple vulnerability sources, as specified in Requirement 6.3.1. Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities were resolved as part of the three-month vulnerability scan cycle. However, additional documentation may be required to verify non-remediated vulnerabilities are in the process of being resolved. While scans are required at least once every three months, more frequent scans are recommended depending on the network complexity, frequency of change, and types of devices, software, and operating systems used. *(continued on next page)*
11.3.1 Internal vulnerability scans are performed as follows: • At least once every three months. • Vulnerabilities that are either high-risk or critical (according to the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved. • Rescans are performed that confirm all high-risk and all critical vulnerabilities (as noted above) have been resolved. • Scan tool is kept up to date with latest vulnerability information. • Scans are performed by qualified personnel and organizational independence of the tester exists.	**11.3.1.a** Examine internal scan report results from the last 12 months to verify that internal scans occurred at least once every three months in the most recent 12-month period.	
	11.3.1.b Examine internal scan report results from each scan and rescan run in the last 12 months to verify that all high-risk vulnerabilities and all critical vulnerabilities (defined in PCI DSS Requirement 6.3.1) are resolved.	
	11.3.1.c Examine scan tool configurations and interview personnel to verify that the scan tool is kept up to date with the latest vulnerability information.	
	11.3.1.d Interview responsible personnel to verify that the scan was performed by a qualified internal resource(s) or qualified external third party and that organizational independence of the tester exists.	
Customized Approach Objective		
The security posture of all system components is verified periodically using automated tools designed to detect vulnerabilities operating inside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework. *(continued on next page)*		

Exhibit 22A-11

Requirements and Testing Procedures		Guidance
Applicability Notes It is not required to use a QSA or ASV to conduct internal vulnerability scans. Internal vulnerability scans can be performed by qualified, internal staff that are reasonably independent of the system component(s) being scanned (for example, a network administrator should not be responsible for scanning the network), or an entity may choose to have internal vulnerability scans performed by a firm specializing in vulnerability scanning.		**Definitions** A vulnerability scan is a combination of automated tools, techniques, and/or methods run against external and internal devices and servers, designed to expose potential vulnerabilities in applications, operating systems, and network devices that could be found and exploited by malicious individuals.

Exhibit 22A-11

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** All vulnerabilities, regardless of criticality, provide a potential avenue of attack and must therefore be addressed periodically, with the vulnerabilities that expose the most risk addressed more quickly to limit the potential window of attack.
11.3.1.1 All other applicable vulnerabilities (those not ranked as high-risk vulnerabilities or critical vulnerabilities according to the entity's vulnerability risk rankings defined at Requirement 6.3.1) are managed as follows: • Addressed based on the risk defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. • Rescans are conducted as needed.	**11.3.1.1.a** Examine the entity's targeted risk analysis that defines the risk for addressing all other applicable vulnerabilities (those not ranked as high-risk vulnerabilities or critical vulnerabilities according to the entity's vulnerability risk rankings at Requirement 6.3.1) to verify the risk analysis was performed in accordance with all elements specified at Requirement 12.3.1.	
	11.3.1.1.b Interview responsible personnel and examine internal scan report results or other documentation to verify that all other applicable vulnerabilities (those not ranked as high-risk vulnerabilities or critical vulnerabilities according to the entity's vulnerability risk rankings at Requirement 6.3.1) are addressed based on the risk defined in the entity's targeted risk analysis, and that the scan process includes rescans as needed to confirm the vulnerabilities have been addressed.	
Customized Approach Objective		
Lower ranked vulnerabilities (lower than high-risk or critical) are addressed at a frequency in accordance with the entity's risk.		
Applicability Notes		
The timeframe for addressing lower-risk vulnerabilities is subject to the results of a risk analysis per Requirement 12.3.1 that includes (minimally) identification of assets being protected, threats, and likelihood and/or impact of a threat being realized. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

Exhibit 22A-11

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Authenticated scanning provides greater insight into an entity's vulnerability landscape since it can detect vulnerabilities that unauthenticated scans cannot detect. Attackers may leverage vulnerabilities that an entity is unaware of because certain vulnerabilities will only be detected with authenticated scanning. Authenticated scanning can yield significant additional information about an organization's vulnerabilities. **Good Practice** The credentials used for these scans should be considered highly privileged. They should be protected and controlled as such, following PCI DSS Requirements 7 and 8 (except for those requirements for multi-factor authentication and application and system accounts).
11.3.1.2 Internal vulnerability scans are performed via authenticated scanning as follows: • Systems that are unable to accept credentials for authenticated scanning are documented. • Sufficient privileges are used for those systems that accept credentials for scanning. • If accounts used for authenticated scanning can be used for interactive login, they are managed in accordance with Requirement 8.2.2.	**11.3.1.2.a** Examine scan tool configurations to verify that authenticated scanning is used for internal scans, with sufficient privileges, for those systems that accept credentials for scanning. **11.3.1.2.b** Examine scan report results and interview personnel to verify that authenticated scans are performed. **11.3.1.2.c** If accounts used for authenticated scanning can be used for interactive login, examine the accounts and interview personnel to verify the accounts are managed following all elements specified in Requirement 8.2.2. **11.3.1.2.d** Examine documentation to verify that systems that are unable to accept credentials for authenticated scanning are defined.	
Customized Approach Objective		
Automated tools used to detect vulnerabilities can detect vulnerabilities local to each system, which are not visible remotely.		
Applicability Notes		
The authenticated scanning tools can be either host-based or network-based. "Sufficient" privileges are those needed to access system resources such that a thorough scan can be conducted that detects known vulnerabilities. This requirement does not apply to system components that cannot accept credentials for scanning. Examples of systems that may not accept credentials for scanning include some network and security appliances, mainframes, and containers. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

Exhibit 22A-11

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Scanning an environment after any significant changes ensures that changes were completed appropriately such that the security of the environment was not compromised because of the change. **Good Practice** Entities should perform scans after significant changes as part of the change process per Requirement 6.5.2 and before considering the change complete. All system components affected by the change will need to be scanned.
11.3.1.3 Internal vulnerability scans are performed after any significant change as follows: • Vulnerabilities that are either high-risk or critical (according to the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved. • Rescans are conducted as needed. • Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).	**11.3.1.3.a** Examine change control documentation and internal scan reports to verify that system components were scanned after any significant changes.	
	11.3.1.3.b Interview personnel and examine internal scan and rescan reports to verify that internal scans were performed after significant changes and that all high-risk vulnerabilities and all critical vulnerabilities (defined in PCI DSS Requirement 6.3.1) were resolved.	
Customized Approach Objective	**11.3.1.3.c** Interview personnel to verify that internal scans are performed by a qualified internal resource(s) or qualified external third party and that organizational independence of the tester exists.	
The security posture of all system components is verified following significant changes to the network or systems, by using automated tools designed to detect vulnerabilities operating inside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.		
Applicability Notes		
Authenticated internal vulnerability scanning per Requirement 11.3.1.2 is not required for scans performed after significant changes.		

Exhibit 22A-11

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Attackers routinely look for unpatched or vulnerable externally facing servers, which can be leveraged to launch a directed attack. Organizations must ensure these externally facing devices are regularly scanned for weaknesses and that vulnerabilities are patched or remediated to protect the entity. Because external networks are at greater risk of compromise, external vulnerability scanning must be performed at least once every three months by a PCI SSC Approved Scanning Vendor (ASV). **Good Practice** While scans are required at least once every three months, more frequent scans are recommended depending on the network complexity, frequency of change, and types of devices, software, and operating systems used. Vulnerabilities identified during external vulnerability scans should be part of a vulnerability management process that includes multiple vulnerability sources, as specified in Requirement 6.3.1. Multiple scan reports can be combined to show that all systems were scanned and that all applicable vulnerabilities were resolved as part of the three-month vulnerability scan cycle. However, additional documentation may be required to verify non-remediated vulnerabilities are in the process of being resolved. **Further Information** See the *ASV Program Guide* on the PCI SSC website.
11.3.2 External vulnerability scans are performed as follows: • At least once every three months. • By a PCI SSC Approved Scanning Vendor (ASV). • Vulnerabilities are resolved and *ASV Program Guide* requirements for a passing scan are met. • Rescans are performed as needed to confirm that vulnerabilities are resolved per the *ASV Program Guide* requirements for a passing scan.	**11.3.2.a** Examine ASV scan reports from the last 12 months to verify that external vulnerability scans occurred at least once every three months in the most recent 12-month period. **11.3.2.b** Examine the ASV scan report from each scan and rescan run in the last 12 months to verify that vulnerabilities are resolved and the *ASV Program Guide* requirements for a passing scan are met. **11.3.2.c** Examine the ASV scan reports to verify that the scans were completed by a PCI SSC Approved Scanning Vendor (ASV).	
Customized Approach Objective		
This requirement is not eligible for the customized approach.		
Applicability Notes		
For the initial PCI DSS assessment against this requirement, it is not required that four passing scans be completed within 12 months if the assessor verifies: 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring scanning at least once every three months, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). *(continued on next page)*		

Exhibit 22A-11

Requirements and Testing Procedures		Guidance
However, for subsequent years after the initial PCI DSS assessment, passing scans at least every three months must have occurred. ASV scanning tools can scan a vast array of network types and topologies. Any specifics about the target environment (for example, load balancers, third-party providers, ISPs, specific configurations, protocols in use, scan interference) should be worked out between the ASV and scan customer. Refer to the *ASV Program Guide* published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.		

Exhibit 22A-11

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Scanning an environment after any significant changes ensures that changes were completed appropriately such that the security of the environment was not compromised because of the change. **Good Practice** Entities should include the need to perform scans after significant changes as part of the change process and before the change is considered complete. All system components affected by the change will need to be scanned.
11.3.2.1 External vulnerability scans are performed after any significant change as follows: • Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved. • Rescans are conducted as needed. • Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).	**11.3.2.1.a** Examine change control documentation and external scan reports to verify that system components were scanned after any significant changes.	
	11.3.2.1.b Interview personnel and examine external scan and rescan reports to verify that external scans were performed after significant changes and that vulnerabilities scored 4.0 or higher by the CVSS were resolved.	
Customized Approach Objective	**11.3.2.1.c** Interview personnel to verify that external scans are performed by a qualified internal resource(s) or qualified external third party and that organizational independence of the tester exists.	
The security posture of all system components is verified following significant changes to the network or systems, by using tools designed to detect vulnerabilities operating from outside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.		

Exhibit 22A-11

Requirements and Testing Procedures		Guidance
11.4 External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Attackers spend a lot of time finding external and internal vulnerabilities to leverage to obtain access to cardholder data and then to exfiltrate that data. As such, entities need to test their networks thoroughly, just as an attacker would do. This testing allows the entity to identify and remediate weakness that might be leveraged to compromise the entity's network and data, and then to take appropriate actions to protect the network and system components from such attacks. **Good Practice** Penetration testing techniques will differ based on an organization's needs and structure and should be suitable for the tested environment—for example, fuzzing, injection, and forgery tests might be appropriate. The type, depth, and complexity of the testing will depend on the specific environment and the needs of the organization. **Definitions** Penetration tests simulate a real-world attack situation intending to identify how far an attacker could penetrate an environment, given differing amounts of information provided to the tester. This allows an entity to better understand its potential exposure and develop a strategy to defend against attacks. A penetration test differs from a vulnerability scan, as a penetration test is an active process that usually includes exploiting identified vulnerabilities. *(continued on next page)*
11.4.1 A penetration testing methodology is defined, documented, and implemented by the entity, and includes: • Industry-accepted penetration testing approaches. • Coverage for the entire CDE perimeter and critical systems. • Testing from both inside and outside the network. • Testing to validate any segmentation and scope-reduction controls. • Application-layer penetration testing to identify, at a minimum, the vulnerabilities listed in Requirement 6.2.4. • Network-layer penetration tests that encompass all components that support network functions as well as operating systems. • Review and consideration of threats and vulnerabilities experienced in the last 12 months. • Documented approach to assessing and addressing the risk posed by exploitable vulnerabilities and security weaknesses found during penetration testing. Retention of penetration testing results and remediation activities results for at least 12 months.	**11.4.1** Examine documentation and interview personnel to verify that the penetration-testing methodology defined, documented, and implemented by the entity includes all elements specified in this requirement.	

Exhibit 22A-11

Requirements and Testing Procedures		Guidance
Customized Approach Objective A formal methodology is defined for thorough technical testing that attempts to exploit vulnerabilities and security weaknesses via simulated attack methods by a competent manual attacker. **Applicability Notes** Testing from inside the network (or “internal penetration testing”) means testing from both inside the CDE and into the CDE from trusted and untrusted internal networks. Testing from outside the network (or “external penetration testing”) means testing the exposed external perimeter of trusted networks, and critical systems connected to or accessible to public network infrastructures.		Scanning for vulnerabilities alone is not a penetration test, nor is a penetration test adequate if the focus is solely on trying to exploit vulnerabilities found in a vulnerability scan. Conducting a vulnerability scan may be one of the first steps, but it is not the only step a penetration tester will perform to plan the testing strategy. Even if a vulnerability scan does not detect known vulnerabilities, the penetration tester will often gain enough knowledge about the system to identify possible security gaps. Penetration testing is a highly manual process. While some automated tools may be used, the tester uses their knowledge of systems to gain access into an environment. Often the tester will chain several types of exploits together with the goal of breaking through layers of defenses. For example, if the tester finds a way to gain access to an application server, the tester will then use the compromised server as a point to stage a new attack based on the resources to which the server has access. In this way, a tester can simulate the techniques used by an attacker to identify areas of potential weakness in the environment. The testing of security monitoring and detection methods—for example, to confirm the effectiveness of logging and file integrity monitoring mechanisms, should also be considered. *(continued on next page)*

Exhibit 22A-11

Requirements and Testing Procedures		Guidance
11.4.1 *(continued)*		**Further Information** Refer to the *Information Supplement: Penetration Testing Guidance* for additional guidance. Industry-accepted penetration testing approaches include: *The Open Source Security Testing Methodology and Manual (OSSTMM)* *Open Web Application Security Project (OWASP) penetration testing programs.*
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Internal penetration testing serves two purposes. Firstly, just like an external penetration test, it discovers vulnerabilities and misconfigurations that could be used by an attacker that had managed to get some degree of access to the internal network, whether that is because the attacker is an authorized user conducting unauthorized activities, or an external attacker that had managed to penetrate the entity's perimeter. Secondly, internal penetration testing also helps entities to discover where their change control process failed by detecting previously unknown systems. Additionally, it verifies the status of many of the controls operating within the CDE. A penetration test is not truly a "test" because the outcome of a penetration test is not something that can be classified as a "pass" or a "fail." The best outcome of a test is a catalog of vulnerabilities and misconfigurations that an entity
11.4.2 Internal penetration testing is performed: • Per the entity's defined methodology, • At least once every 12 months • After any significant infrastructure or application upgrade or change • By a qualified internal resource or qualified external third-party • Organizational independence of the tester exists (not required to be a QSA or ASV).	**11.4.2.a** Examine the scope of work and results from the most recent internal penetration test to verify that penetration testing is performed in accordance with all elements specified in this requirement.	
	11.4.2.b Interview personnel to verify that the internal penetration test was performed by a qualified internal resource or qualified external third-party and that organizational independence of the tester exists (not required to be a QSA or ASV).	
Customized Approach Objective		
Internal system defenses are verified by technical testing according to the entity's defined methodology as frequently as needed to address evolving and new attacks and threats and ensure that significant changes do not introduce unknown vulnerabilities.		

Exhibit 22A-11

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	did not know about, and the penetration tester found them before an attacker could. A penetration test that found nothing is typically indicative of shortcomings of the penetration tester, rather than being a positive reflection of the security posture of the entity. **Good Practice** Some considerations when choosing a qualified resource to perform penetration testing include: • Specific penetration testing certifications, which may be an indication of the tester's skill level and competence. • Prior experience conducting penetration testing—for example, the number of years of experience, and the type and scope of prior engagements can help confirm whether the tester's experience is appropriate for the needs of the engagement. **Further Information** Refer to the *Information Supplement: Penetration Testing Guidance* on the PCI SSC website for additional guidance.
11.4.3 External penetration testing is performed: • Per the entity's defined methodology • At least once every 12 months • After any significant infrastructure or application upgrade or change • By a qualified internal resource or qualified external third party • Organizational independence of the tester exists (not required to be a QSA or ASV)	**11.4.3.a** Examine the scope of work and results from the most recent external penetration test to verify that penetration testing is performed according to all elements specified in this requirement.	
	11.4.3.b Interview personnel to verify that the external penetration test was performed by a qualified internal resource or qualified external third party and that organizational independence of the tester exists (not required to be a QSA or ASV).	
Customized Approach Objective		
External system defenses are verified by technical testing according to the entity's defined methodology as frequently as needed to address evolving and new attacks and threats, and to ensure that significant changes do not introduce unknown vulnerabilities.		

Exhibit 22A-11

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** The results of a penetration test are usually a prioritized list of vulnerabilities discovered by the exercise. Often a tester will have chained a number of vulnerabilities together to compromise a system component. Remediating the vulnerabilities found by a penetration test significantly reduces the probability that the same vulnerabilities will be exploited by a malicious attacker. Using the entity's own vulnerability risk assessment process (see requirement 6.3.1) ensures that the vulnerabilities that pose the highest risk to the entity will be remediated more quickly. **Good Practice** As part of the entity's assessment of risk, entities should consider how likely the vulnerability is to be exploited and whether there are other controls present in the environment to reduce the risk. Any weaknesses that point to PCI DSS requirements not being met should be addressed.
11.4.4 Exploitable vulnerabilities and security weaknesses found during penetration testing are corrected as follows: • In accordance with the entity's assessment of the risk posed by the security issue as defined in Requirement 6.3.1. • Penetration testing is repeated to verify the corrections.	**11.4.4** Examine penetration testing results to verify that noted exploitable vulnerabilities and security weaknesses were corrected in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Vulnerabilities and security weaknesses found while verifying system defenses are mitigated.		

Exhibit 22A-11

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** When an entity uses segmentation controls to isolate the CDE from internal untrusted networks, the security of the CDE is dependent on that segmentation functioning. Many attacks have involved the attacker moving laterally from what an entity deemed an isolated network into the CDE. Using penetration testing tools and techniques to validate that an untrusted network is indeed isolated from the CDE can alert the entity to a failure or misconfiguration of the segmentation controls, which can then be rectified. **Good Practice** Techniques such as host discovery and port scanning can be used to verify out-of-scope segments have no access to the CDE.
11.4.5 If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: • At least once every 12 months and after any changes to segmentation controls/methods • Covering all segmentation controls/methods in use. • According to the entity's defined penetration testing methodology. • Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. • Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). • Performed by a qualified internal resource or qualified external third party. • Organizational independence of the tester exists (not required to be a QSA or ASV).	**11.4.5.a** Examine segmentation controls and review penetration-testing methodology to verify that penetration-testing procedures are defined to test all segmentation methods in accordance with all elements specified in this requirement.	
	11.4.5.b Examine the results from the most recent penetration test to verify the penetration test covers and addresses all elements specified in this requirement.	
	11.4.5.c Interview personnel to verify that the test was performed by a qualified internal resource or qualified external third party and that organizational independence of the tester exists (not required to be a QSA or ASV).	
Customized Approach Objective		
If segmentation is used, it is verified periodically by technical testing to be continually effective, including after any changes, in isolating the CDE from all out-of-scope systems.		

Exhibit 22A-11

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Service providers typically have access to greater volumes of cardholder data or can provide an entry point that can be exploited to then compromise multiple other entities. Service providers also typically have larger and more complex networks that are subject to more frequent change. The probability of segmentation controls failing in complex and dynamic networks is greater in service-provider environments. Validating segmentation controls more frequently is likely to discover such failings before they can be exploited by an attacker attempting to pivot laterally from an out-of-scope untrusted network to the CDE. **Good Practice** Although the requirement specifies that this scope validation is carried out at least once every six months and after significant change, this exercise should be performed as frequently as possible to ensure it remains effective at isolating the CDE from other networks.
11.4.6 ***Additional requirement for service providers only:*** If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: • At least once every six months and after any changes to segmentation controls/methods. • Covering all segmentation controls/methods in use. • According to the entity's defined penetration testing methodology. • Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. • Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). • Performed by a qualified internal resource or qualified external third party. • Organizational independence of the tester exists (not required to be a QSA or ASV).	**11.4.6.a** ***Additional testing procedure for service provider assessments only:*** Examine the results from the most recent penetration test to verify that the penetration covers and addressed all elements specified in this requirement. **11.4.6.b** ***Additional testing procedure for service provider assessments only:*** Interview personnel to verify that the test was performed by a qualified internal resource or qualified external third party and that organizational independence of the tester exists (not required to be a QSA or ASV).	
Customized Approach Objective		
If segmentation is used, it is verified by technical testing to be continually effective, including after any changes, in isolating the CDE from out-of-scope systems.		
Applicability Notes		
This requirement applies only when the entity being assessed is a service provider.		

Exhibit 22A-11

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Entities need to conduct penetration tests in accordance with PCI DSS to simulate attacker behavior and discover vulnerabilities in their environment. In shared and cloud environments, the multi-tenant service provider may be concerned about the activities of a penetration tester affecting other customers' systems. Multi-tenant service providers cannot forbid penetration testing because this would leave their customers' systems open to exploitation. Therefore, multi-tenant service providers must support customer requests to conduct penetration testing or for penetration testing results.
11.4.7 *Additional requirement for multi-tenant service providers only:* Multi-tenant service providers support their customers for external penetration testing per Requirement 11.4.3 and 11.4.4.	**11.4.7 *Additional testing procedure for multi-tenant service providers only:*** Examine evidence to verify that multi-tenant service providers support their customers for external penetration testing per Requirement 11.4.3 and 11.4.4.	
Customized Approach Objective		
Multi-tenant service providers support their customers' need for technical testing either by providing access or evidence that comparable technical testing has been undertaken. *(continued on next page)*		

Exhibit 22A-11

Requirements and Testing Procedures		Guidance
Applicability Notes		
This requirement applies only when the entity being assessed is a multi-tenant service provider. To meet this requirement, a multi-tenant service provider may either: • Provide evidence to its customers to show that penetration testing has been performed according to Requirements 11.4.3 and 11.4.4 on the customers' subscribed infrastructure, or • Provide prompt access to each of its customers, so customers can perform their own penetration testing. Evidence provided to customers can include redacted penetration testing results but needs to include sufficient information to prove that all elements of Requirements 11.4.3 and 11.4.4 have been met on the customer's behalf. Refer also to *Appendix A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers*. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

Exhibit 22A-11

Requirements and Testing Procedures		Guidance
11.5 Network intrusions and unexpected file changes are detected and responded to.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Intrusion-detection and/or intrusion-prevention techniques (such as IDS/IPS) compare the traffic coming into the network with known "signatures" and/or behaviors of thousands of compromise types (hacker tools, Trojans, and other malware), and then send alerts and/or stop the attempt as it happens. Without a proactive approach to detect unauthorized activity, attacks on (or misuse of) computer resources could go unnoticed for long periods of time. The impact of an intrusion into the CDE is, in many ways, a factor of the time that an attacker has in the environment before being detected. **Good Practice** Security alerts generated by these techniques should be continually monitored, so that the attempted or actual intrusions can be stopped, and potential damage limited. **Definitions** Critical locations could include, but are not limited to, network security controls between network segments (for example, between a DMZ and an internal network or between an in-scope and out-of-scope network) and points protecting connections between a less trusted and a more trusted system component.
11.5.1 Intrusion-detection and/or intrusion-prevention techniques are used to detect and/or prevent intrusions into the network as follows: • All traffic is monitored at the perimeter of the CDE. • All traffic is monitored at critical points in the CDE. • Personnel are alerted to suspected compromises. • All intrusion-detection and prevention engines, baselines, and signatures are kept up to date.	**11.5.1.a** Examine system configurations and network diagrams to verify that intrusion-detection and/or intrusion-prevention techniques are in place to monitor all traffic: • At the perimeter of the CDE. • At critical points in the CDE.	
	11.5.1.b Examine system configurations and interview responsible personnel to verify intrusion-detection and/or intrusion-prevention techniques alert personnel of suspected compromises.	
Customized Approach Objective Mechanisms to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity are implemented. Alerts generated by these mechanisms are responded to by personnel, or by automated means that ensure that system components cannot be compromised as a result of the detected activity.	**11.5.1.c** Examine system configurations and vendor documentation to verify intrusion-detection and/or intrusion-prevention techniques are configured to keep all engines, baselines, and signatures up to date.	

Exhibit 22A-11

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Detecting covert malware communication attempts (for example, DNS tunneling) can help block the spread of malware laterally inside a network and the exfiltration of data. When deciding where to place this control, entities should consider critical locations in the network, and likely routes for covert channels. When malware establishes a foothold in an infected environment, it often tries to establish a communication channel to a command-and-control (C&C) server. Through the C&C server, the attacker communicates with and controls malware on compromised systems to deliver malicious payloads or instructions, or to initiate data exfiltration. In many cases, the malware will communicate with the C&C server indirectly via botnets, bypassing monitoring, blocking controls, and rendering these methods ineffective to detect the covert channels. *(continued on next page)*
11.5.1.1 ***Additional requirement for service providers only:*** Intrusion-detection and/or intrusion-prevention techniques detect, alert on/prevent, and address covert malware communication channels.	**11.5.1.1.a** ***Additional testing procedure for service provider assessments only:*** Examine documentation and configuration settings to verify that methods to detect and alert on/prevent covert malware communication channels are in place and operating.	
	11.5.1.1.b ***Additional testing procedure for service provider assessments only:*** Examine the entity's incident-response plan (Requirement 12.10.1) to verify it requires and defines a response in the event that covert malware communication channels are detected.	
Customized Approach Objective	**11.5.1.1.c** ***Additional testing procedure for service provider assessments only:*** Interview responsible personnel and observe processes to verify that personnel maintain knowledge of covert malware communication and control techniques and are knowledgeable about how to respond when malware is suspected.	
Mechanisms are in place to detect and alert/prevent covert communications with command-and-control systems. Alerts generated by these mechanisms are responded to by personnel, or by automated means that ensure that such communications are blocked. *(continued on next page)*		

Exhibit 22A-11

Requirements and Testing Procedures		Guidance
Applicability Notes This requirement applies only when the entity being assessed is a service provider. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		**Good Practice** Methods that can help detect and address malware communications channels include real-time endpoint scanning, egress traffic filtering, an ”allow” listing, data loss prevention tools, and network security monitoring tools such as IDS/IPS. Additionally, DNS queries and responses are a key data source used by network defenders in support of incident response as well as intrusion discovery. When these transactions are collected for processing and analytics, they can enable a number of valuable security analytic scenarios. It is important that organizations maintain up-to-date knowledge of malware modes of operation, as mitigating these can help detect and limit the impact of malware in the environment.

Exhibit 22A-12

Maintain an Information Security Policy

Requirement 12: Support Information Security with Organizational Policies and Programs

Sections

12.1 A comprehensive information security policy that governs and provides direction for protection of the entity's information assets is known and current.

12.2 Acceptable use policies for end-user technologies are defined and implemented.

12.3 Risks to the cardholder data environment are formally identified, evaluated, and managed.

12.4 PCI DSS compliance is managed.

12.5 PCI DSS scope is documented and validated.

12.6 Security awareness education is an ongoing activity.

12.7 Personnel are screened to reduce risks from insider threats.

12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed.

12.9 Third-party service providers (TPSPs) support their customers' PCI DSS compliance.

12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately.

Overview

The organization's overall information security policy sets the tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of cardholder data and their responsibilities for protecting it.

For the purposes of Requirement 12, "personnel" refers to full-time and part-time employees, temporary employees, contractors, and consultants with security responsibilities for protecting account data or that can impact the security of cardholder data and/or sensitive authentication data.

Refer to *Appendix G* for definitions of PCI DSS terms.

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
12.1 A comprehensive information security policy that governs and provides direction for protection of the entity's information assets is known and current.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** An organization's overall information security policy ties to and governs all other policies and procedures that define protection of cardholder data. The information security policy communicates management's intent and objectives regarding the protection of its most valuable assets, including cardholder data. Without an information security policy, individuals will make their own value decisions on the controls that are required within the organization which may result in the organization neither meeting its legal, regulatory, and contractual obligations, nor being able to adequately protect its assets in a consistent manner. To ensure the policy is implemented, it is important that all relevant personnel within the organization, as well as relevant third parties, vendors, and business partners are aware of the organization's information security policy and their responsibilities for protecting information assets. *(continued on next page)*
12.1.1 An overall information security policy is: • Established. • Published. • Maintained. • Disseminated to all relevant personnel, as well as to relevant vendors and business partners.	**12.1.1** Examine the information security policy and interview personnel to verify that the overall information security policy is managed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
The strategic objectives and principles of information security are defined, adopted, and known to all personnel.		

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
12.1.1 *(continued)*		**Good Practice** The security policy for the organization identifies the purpose, scope, accountability, and information that clearly defines the organization's position regarding information security. The overall information security policy differs from individual security policies that address specific technology or security disciplines. This policy sets forth the directives for the entire organization whereas individual security policies align and support the overall security policy and communicate specific objectives for technology or security disciplines. It is important that all relevant personnel within the organization, as well as relevant third parties, vendors, and business partners are aware of the organization's information security policy and their responsibilities for protecting information assets. **Definitions** "Relevant" for this requirement means that the information security policy is disseminated to those with roles applicable to some or all the topics in the policy, either within the company or because of services/functions performed by a vendor or third party.

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Security threats and associated protection methods evolve rapidly. Without updating the information security policy to reflect relevant changes, new measures to defend against these threats may not be addressed.
12.1.2 The information security policy is: • Reviewed at least once every 12 months. • Updated as needed to reflect changes to business objectives or risks to the environment.	**12.1.2** Examine the information security policy and interview responsible personnel to verify the policy is managed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
The information security policy continues to reflect the organization’s strategic objectives and principles.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Without clearly defined security roles and responsibilities assigned, there could be misuse of the organization’s information assets or inconsistent interaction with information security personnel, leading to insecure implementation of technologies or use of outdated or insecure technologies.
12.1.3 The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities.	**12.1.3.a** Examine the information security policy to verify that they clearly define information security roles and responsibilities for all personnel.	
	12.1.3.b Interview personnel in various roles to verify they understand their information security responsibilities.	
	12.1.3.c Examine documented evidence to verify personnel acknowledge their information security responsibilities.	
Customized Approach Objective		
Personnel understand their role in protecting the entity’s cardholder data.		

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** To ensure someone with sufficient authority and responsibility is actively managing and championing the organization's information security program, accountability and responsibility for information security needs to be assigned at the executive level within an organization. **Good Practice** These executive management positions are often at the most senior level of management and are part of the chief executive level or C-level, typically reporting to the Chief Executive Officer or the Board of Directors. Information security knowledge for this executive management role can be indicated by work experience, education, and/or relevant professional certifications. The expectation is that this individual can provide assurance about the implementation of an effective security program and ensure the right technical experts are employed. Entities should also consider transition and/or succession plans for these key personnel to avoid potential gaps in critical security activities.
12.1.4 Responsibility for information security is formally assigned to a Chief Information Security Officer or other information security knowledgeable member of executive management. .	**12.1.4** Examine the information security policy to verify that information security is formally assigned to a Chief Information Security Officer or other information security-knowledgeable member of executive management.	
Customized Approach Objective		
A designated member of executive management is responsible for information security.		

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
12.2 Acceptable use policies for end-user technologies are defined and implemented.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** End-user technologies are a significant investment and may pose significant risk to an organization if not managed properly. Acceptable use policies outline the expected behavior from personnel when using the organization's information technology and reflect the organization's risk tolerance These policies instruct personnel on what they can and cannot do with company equipment and instruct personnel on correct and incorrect uses of company Internet and email resources. Such policies can legally protect an organization and allow it to act when the policies are violated. **Good Practice** It is important that usage policies are supported by technical controls to manage the enforcement of the policies. Structuring polices as simple "do" and "do not" requirements that are linked to a purpose can help remove ambiguity and provide personnel with the context for the requirement.
12.2.1 Acceptable use policies for end-user technologies are documented and implemented, including: • Explicit approval by authorized parties. • Acceptable uses of the technology. • List of products approved by the company for employee use, including hardware and software.	**12.2.1** Examine the acceptable use policies for end-user technologies and interview responsible personnel to verify processes are documented and implemented in accordance with all elements specified in this requirement.	
Customized Approach Objective		
The use of end-user technologies is defined and managed to ensure authorized usage.		
Applicability Notes		
Examples of end-user technologies for which acceptable use policies are expected include, but are not limited to, remote access and wireless technologies, laptops, tablets, mobile phones, and removable electronic media, email usage, and Internet usage.		

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
12.3 Risks to the cardholder data environment are formally identified, evaluated, and managed.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Some PCI DSS requirements allow an entity to define how frequently an activity is performed based on the risk to the entity's environment. Performing this risk analysis according to a methodology ensures validity and consistency with policies and procedures. This targeted risk analysis (as opposed to a traditional enterprise-wide risk assessment) focuses on those PCI DSS requirements that allow an entity flexibility about how frequently an entity performs a given control. For this risk analysis, the entity carefully evaluates each PCI DSS requirement that provides this flexibility and determines the frequency that supports adequate security for the entity, and the level of risk the entity is willing to accept. The risk analysis identifies the specific assets, such as the system components and data—for example, log files, or credentials—that the requirement is intended to protect, as well as the threat(s) or outcomes that the requirement is protecting the assets from—for example, malware, an undetected intruder, or misuse of credentials. Examples of factors that could contribute to likelihood or impact include any that could increase the vulnerability of an asset to a threat—for example, exposure to untrusted networks, complexity of environment, or high staff turnover—as well as the criticality of the system components, or volume and sensitivity of the data, being protected. *(continued on next page)*
12.3.1 For each PCI DSS requirement that specifies completion of a targeted risk analysis, the analysis is documented and includes: • Identification of the assets being protected. • Identification of the threat(s) that the requirement is protecting against. • Identification of factors that contribute to the likelihood and/or impact of a threat being realized. • Resulting analysis that determines, and includes justification for, how the frequency or processes defined by the entity to meet the requirement minimize the likelihood and/or impact of the threat being realized. • Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed. • Performance of updated risk analyses when needed, as determined by the annual review.	**12.3.1** Examine documented policies and procedures to verify a process is defined for performing targeted risk analyses for each PCI DSS requirement that specifies completion of a targeted risk analysis, and that the process includes all elements specified in this requirement.	
Customized Approach Objective		
Up to date knowledge and assessment of risks to the CDE are maintained.		
Applicability Notes		
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.		

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
12.3.1 *(continued)*		Reviewing the results of these targeted risk analyses at least once every 12 months and upon changes that could impact the risk to the environment allows the organization to ensure the risk analysis results remain current with organizational changes and evolving threats, trends, and technologies, and that the selected frequencies still adequately address the entity's risk. **Good Practice** An enterprise-wide risk assessment, which is a point-in-time activity that enables entities to identify threats and associated vulnerabilities, is recommended, but is not required, for entities to determine and understand broader and emerging threats with the potential to negatively impact its business. This enterprise-wide risk assessment could be established as part of an overarching risk management program that is used as an input to the annual review of an organization's overall information security policy (see Requirement 12.1.1). Examples of risk-assessment methodologies for enterprise-wide risk assessments include, but are not limited to, ISO *27005* and NIST *SP 800-30*. **Further Information** Refer to the following documents on the PCI SSC website: • *Information Supplement: TRA Guidance* • *Sample Template: TRA for Activity Frequency*.

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** A risk analysis following a repeatable and robust methodology enables an entity to meet the customized approach objective. **Definitions** The customized approach to meeting a PCI DSS requirement allows entities to define the controls used to meet a given requirement's stated Customized Approach Objective in a way that does not strictly follow the defined requirement. These controls are expected to at least meet or exceed the security provided by the defined requirement and require extensive documentation by the entity using the customized approach. **Further Information** See *Appendix D: Customized Approach* for instructions on how to document the required evidence for the customized approach. See *PCI DSS v4.x: Sample Templates to Support Customized Approach* on the PCI SSC website for templates that entities may use to document their customized controls. Note that while use of the templates is optional, the information specified within each template must be documented and provided to each entity's assessor.
12.3.2 A targeted risk analysis is performed for each PCI DSS requirement that the entity meets with the customized approach, to include: • Documented evidence detailing each element specified in Appendix D: Customized Approach (including, at a minimum, a controls matrix and risk analysis). • Approval of documented evidence by senior management. • Performance of the targeted analysis of risk at least once every 12 months.	**12.3.2** Examine the documented targeted risk-analysis for each PCI DSS requirement that the entity meets with the customized approach to verify that documentation for each requirement exists and is in accordance with all elements specified in this requirement.	
Customized Approach Objective		
This requirement is part of the customized approach and must be met for those using the customized approach.		
Applicability Notes		
This requirement only applies to entities using a Customized Approach.		

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Protocols and encryption strengths may quickly change or be deprecated due to identification of vulnerabilities or design flaws. In order to support current and future data security needs, entities need to know where cryptography is used and understand how they would be able to respond rapidly to changes impacting the strength of their cryptographic implementations. **Good Practice** Cryptographic agility is important to ensure an alternative to the original encryption method or cryptographic primitive is available, with plans to upgrade to the alternative without significant change to system infrastructure. For example, if the entity is aware of when protocols or algorithms will be deprecated by standards bodies, proactive plans will help the entity to upgrade before the deprecation is impactful to operations. **Definitions** “Cryptographic agility” refers to the ability to monitor and manage the encryption and related verification technologies deployed across an organization. **Further Information** Refer to *NIST SP 800-131a, Transitioning the Use of Cryptographic Algorithms and Key Lengths*.
12.3.3 Cryptographic cipher suites and protocols in use are documented and reviewed at least once every 12 months, including at least the following: • An up-to-date inventory of all cryptographic cipher suites and protocols in use, including purpose and where used. • Active monitoring of industry trends regarding continued viability of all cryptographic cipher suites and protocols in use. • Documentation of a plan, to respond to anticipated changes in cryptographic vulnerabilities.	**12.3.3** Examine documentation for cryptographic suites and protocols in use and interview personnel to verify the documentation and review is in accordance with all elements specified in this requirement.	
Customized Approach Objective		
The entity is able to respond quickly to any vulnerabilities in cryptographic protocols or algorithms, where those vulnerabilities affect protection of cardholder data.		
Applicability Notes		
The requirement applies to all cryptographic cipher suites and protocols used to meet PCI DSS requirements, including, but not limited to, those used to render PAN unreadable in storage and transmission, to protect passwords, and as part of authenticating access. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Hardware and software technologies are constantly evolving, and organizations need to be aware of changes to the technologies they use, as well as the evolving threats to those technologies to ensure that they can prepare for, and manage, vulnerabilities in hardware and software that will not be remediated by the vendor or developer. **Good Practice** Organizations should review firmware versions to ensure they remain current and supported by the vendors. Organizations also need to be aware of changes made by technology vendors to their products or processes to understand how such changes may impact the organization's use of the technology. Regular reviews of technologies that impact or influence PCI DSS controls can assist with purchasing, usage, and deployment strategies, and ensure controls that rely on those technologies remain effective. These reviews include, but are not limited to, reviewing technologies that are no longer supported by the vendor and/or no longer meet the security needs of the organization.
12.3.4 Hardware and software technologies in use are reviewed at least once every 12 months, including at least the following: • Analysis that the technologies continue to receive security fixes from vendors promptly. • Analysis that the technologies continue to support (and do not preclude) the entity's PCI DSS compliance. • Documentation of any industry announcements or trends related to a technology, such as when a vendor has announced "end of life" plans for a technology. • Documentation of a plan, approved by senior management, to remediate outdated technologies, including those for which vendors have announced "end of life" plans.	**12.3.4** Examine documentation for the review of hardware and software technologies in use and interview personnel to verify that the review is in accordance with all elements specified in this requirement.	
Customized Approach Objective		
The entity's hardware and software technologies are up to date and supported by the vendor. Plans to remove or replace all unsupported system components are reviewed periodically.		
Applicability Notes		
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.		

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
12.4 PCI DSS compliance is managed.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Executive management assignment of PCI DSS compliance responsibilities ensures executive-level visibility into the PCI DSS compliance program and allows for the opportunity to ask appropriate questions to determine the effectiveness of the program and influence strategic priorities.
12.4.1 ***Additional requirement for service providers only:*** Responsibility is established by executive management for the protection of cardholder data and a PCI DSS compliance program to include: • Overall accountability for maintaining PCI DSS compliance. • Defining a charter for a PCI DSS compliance program and communication to executive management.	**12.4.1** ***Additional testing procedure for service provider assessments only:*** Examine documentation to verify that executive management has established responsibility for the protection of cardholder data and a PCI DSS compliance program in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Executives are responsible and accountable for security of cardholder data.		
Applicability Notes		
This requirement applies only when the entity being assessed is a service provider. Executive management may include C-level positions, board of directors, or equivalent. The specific titles will depend on the particular organizational structure. Responsibility for the PCI DSS compliance program may be assigned to individual roles and/or to business units within the organization.		

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	
12.4.2 ***Additional requirement for service providers only:*** Reviews are performed at least once every three months to confirm that personnel are performing their tasks in accordance with all security policies and operational procedures. Reviews are performed by personnel other than those responsible for performing the given task and include, but are not limited to, the following tasks: • Daily log reviews. • Configuration reviews for network security controls. • Applying configuration standards to new systems. • Responding to security alerts. • Change-management processes.	**12.4.2.a** ***Additional testing procedure for service provider assessments only:*** Examine policies and procedures to verify that processes are defined for conducting reviews to confirm that personnel are performing their tasks in accordance with all security policies and all operational procedures, including but not limited to the tasks specified in this requirement. **12.4.2.b** ***Additional testing procedure for service provider assessments only:*** Interview responsible personnel and examine records of reviews to verify that reviews are performed: • At least once every three months. • By personnel other than those responsible for performing the given task.	**Purpose** Regularly confirming that security policies and procedures are being followed provides assurance that the expected controls are active and working as intended. This requirement is distinct from other requirements that specify a task to be performed. The objective of these reviews is not to reperform other PCI DSS requirements, but to confirm that security activities are being performed on an ongoing basis. **Good Practice** These reviews can also be used to verify that appropriate evidence is being maintained—for example, audit logs, vulnerability scan reports, reviews of network security control rulesets—to assist in the entity's preparation for its next PCI DSS assessment. **Examples** Looking at Requirement 1.2.7 as one example, Requirement 12.4.2 is met by confirming, at least once every three months, that reviews of configurations of network security controls have occurred at the required frequency. On the other hand, Requirement 1.2.7 is met by reviewing those configurations as specified in the requirement.
Customized Approach Objective		
The operational effectiveness of critical PCI DSS controls is verified periodically by manual inspection of records.		
Applicability Notes		
This requirement applies only when the entity being assessed is a service provider.		

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** The intent of these independent checks is to confirm whether security activities are being performed on an ongoing basis. These reviews can also be used to verify that appropriate evidence is being maintained—for example, audit logs, vulnerability scan reports, reviews of network security control rulesets—to assist in the entity's preparation for its next PCI DSS assessment.
12.4.2.1 ***Additional requirement for service providers only:*** Reviews conducted in accordance with Requirement 12.4.2 are documented to include: • Results of the reviews. • Documented remediation actions taken for any tasks that were found to not be performed at Requirement 12.4.2. • Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program.	**12.4.2.1** ***Additional testing procedure for service provider assessments only:*** Examine documentation from the reviews conducted in accordance with PCI DSS Requirement 12.4.2 to verify the documentation includes all elements specified in this requirement.	
Customized Approach Objective		
Findings from operational effectiveness reviews are evaluated by management; appropriate remediation activities are implemented.		
Applicability Notes		
This requirement applies only when the entity being assessed is a service provider.		

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
12.5 PCI DSS scope is documented and validated.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Maintaining a current list of all system components will enable an organization to define the scope of its environment and implement PCI DSS requirements accurately and efficiently. Without an inventory, some system components could be overlooked and be inadvertently excluded from the organization's configuration standards. **Good Practice** If an entity keeps an inventory of all assets, those system components in scope for PCI DSS should be clearly identifiable among the other assets. Inventories should include containers or images that may be instantiated. Assigning an owner to the inventory helps to ensure the inventory stays current. **Examples** Methods to maintain an inventory include as a database, as a series of files, or in an inventory-management tool.
12.5.1 An inventory of system components that are in scope for PCI DSS, including a description of function/use, is maintained and kept current.	**12.5.1.a** Examine the inventory to verify it includes all in-scope system components and a description of function/use for each. **12.5.1.b** Interview personnel to verify the inventory is kept current.	
Customized Approach Objective		
All system components in scope for PCI DSS are identified and known.		

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	
12.5.2 PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes: • Identifying all data flows for the various payment stages (for example, authorization, capture settlement, chargebacks, and refunds) and acceptance channels (for example, card-present, card-not-present, and e-commerce). • Updating all data-flow diagrams per Requirement 1.2.4. • Identifying all locations where account data is stored, processed, and transmitted, including but not limited to: 1) any locations outside of the currently defined CDE, 2) applications that process CHD, 3) transmissions between systems and networks, and 4) file backups. • Identifying all system components in the CDE, connected to the CDE, or that could impact security of the CDE. • Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope. • Identifying all connections from third-party entities with access to the CDE. • Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope.	**12.5.2.a** Examine documented results of scope reviews and interview personnel to verify that the reviews are performed: • At least once every 12 months. • After significant changes to the in-scope environment.	**Purpose** Frequent validation of PCI DSS scope helps to ensure PCI DSS scope remains up to date and aligned with changing business objectives, and therefore that security controls are protecting all appropriate system components. **Good Practice** Accurate scoping involves critically evaluating the CDE and all connected system components to determine the necessary coverage for PCI DSS requirements. Scoping activities, including careful analysis and ongoing monitoring, help to ensure that in-scope systems are appropriately secured. When documenting account data locations, the entity can consider creating a table or spreadsheet that includes the following information: • Data stores (databases, files, cloud, etc.), including the purpose of data storage and the retention period, • Which CHD elements are stored (PAN, expiry date, cardholder name, and/or any elements of SAD prior to completion of authorization), • How data is secured (type of encryption and strength, hashing algorithm and strength, truncation, tokenization), • How access to data stores is logged, including a description of logging mechanism(s) in use (enterprise solution, application level, operating system level, etc.). *(continued on next page)*
	12.5.2.b Examine documented results of scope reviews performed by the entity to verify that PCI DSS scoping confirmation activity includes all elements specified in this requirement.	

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
Customized Approach Objective PCI DSS scope is verified periodically, and after significant changes, by comprehensive analysis and appropriate technical measures. **Applicability Notes** This annual confirmation of PCI DSS scope is an activity expected to be performed by the entity under assessment, and is not the same, nor is it intended to be replaced by, the scoping confirmation performed by the entity's assessor during the annual assessment.		In addition to internal systems and networks, all connections from third-party entities—for example, business partners, entities providing remote support services, and other service providers—need to be identified to determine inclusion for PCI DSS scope. Once the in-scope connections have been identified, the applicable PCI DSS controls can be implemented to reduce the risk of a third-party connection being used to compromise an entity's CDE. A data discovery tool or methodology can be used to facilitate identifying all sources and locations of PAN, and to look for PAN that resides on systems and networks outside the currently defined CDE or in unexpected places within the defined CDE—for example, in an error log or memory dump file. This approach can help ensure that previously unknown locations of PAN are detected and that the PAN is either eliminated or properly secured. **Further Information** For additional guidance, refer to *Information Supplement: Guidance for PCI DSS Scoping and Network Segmentation*.

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
12.5.2.1 ***Additional requirement for service providers only:*** PCI DSS scope is documented and confirmed by the entity at least once every six months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes all the elements specified in Requirement 12.5.2.	**12.5.2.1.a** ***Additional testing procedure for service provider assessments only:*** Examine documented results of scope reviews and interview personnel to verify that reviews per Requirement 12.5.2 are performed: • At least once every six months, and • After significant changes	Service providers typically have access to greater volumes of cardholder data than do merchants, or can provide an entry point that can be exploited to then compromise multiple other entities. Service providers also typically have larger and more complex networks that are subject to more frequent change. The probability of overlooked changes to scope in complex and dynamic networks is greater in service-providers environments. Validating PCI DSS scope more frequently is likely to discover such overlooked changes before they can be exploited by an attacker.
	12.5.2.1.b ***Additional testing procedure for service provider assessments only:*** Examine documented results of scope reviews to verify that scoping validation includes all elements specified in Requirement 12.5.2.	
Customized Approach Objective		
The accuracy of PCI DSS scope is verified to be continuously accurate by comprehensive analysis and appropriate technical measures.		
Applicability Notes		
This requirement applies only when the entity being assessed is a service provider. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	
12.5.3 ***Additional requirement for service providers only:*** Significant changes to organizational structure result in a documented (internal) review of the impact to PCI DSS scope and applicability of controls, with results communicated to executive management.	**12.5.3.a** ***Additional testing procedure for service provider assessments only:*** Examine policies and procedures to verify that processes are defined such that a significant change to organizational structure results in documented review of the impact to PCI DSS scope and applicability of controls.	**Purpose** An organization's structure and management define the requirements and protocol for effective and secure operations. Changes to this structure could have negative effects to existing controls and frameworks by reallocating or removing resources that once supported PCI DSS controls or inheriting new responsibilities that may not have established controls in place. Therefore, it is important to revisit PCI DSS scope and controls when there are changes to an organization's structure and management to ensure controls are in place and active. **Examples** Changes to organizational structure include, but are not limited to, company mergers or acquisitions, and significant changes or reassignments of personnel with responsibility for security controls.
Customized Approach Objective PCI DSS scope is confirmed after significant organizational change. **Applicability Notes** This requirement applies only when the entity being assessed is a service provider. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	**12.5.3.b** ***Additional testing procedure for service provider assessments only:*** Examine documentation (for example, meeting minutes) and interview responsible personnel to verify that significant changes to organizational structure resulted in documented reviews that included all elements specified in this requirement, with results communicated to executive management.	

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
12.6 Security awareness education is an ongoing activity.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If personnel are not educated about their company's information security policies and procedures and their own security responsibilities, security safeguards and processes that have been implemented may become ineffective through unintentional errors or intentional actions.
12.6.1 A formal security awareness program is implemented to make all personnel aware of the entity's information security policy and procedures, and their role in protecting the cardholder data.	**12.6.1** Examine the security awareness program to verify it provides awareness to all personnel about the entity's information security policy and procedures, and personnel's role in protecting the cardholder data.	
Customized Approach Objective		
Personnel are knowledgeable about the threat landscape, their responsibility for the operation of relevant security controls, and are able to access assistance and guidance when required.		

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
12.6.2 The security awareness program is: - Reviewed at least once every 12 months, and - Updated as needed to address any new threats and vulnerabilities that may impact the security of the entity's cardholder data and/or sensitive authentication data, or the information provided to personnel about their role in protecting cardholder data.	**12.6.2** Examine security awareness program content, evidence of reviews, and interview personnel to verify that the security awareness program is in accordance with all elements specified in this requirement.	The threat environment and an entity's defenses are not static. As such, the security awareness program materials must be updated as frequently as needed to ensure that the education received by personnel is up to date and represents the current threat environment.
Customized Approach Objective		
The content of security awareness material is reviewed and updated periodically.		
Applicability Notes		
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.		

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Training of personnel ensures they receive the information about the importance of information security and that they understand their role in protecting the organization. Requiring an acknowledgment by personnel helps ensure that they have read and understood the security policies and procedures, and that they have made and will continue to make a commitment to comply with these policies. **Good Practice** Entities may incorporate new-hire training as part of the Human Resources onboarding process. Training should outline the security-related “dos” and “don’ts.” Periodic refresher training reinforces key security processes and procedures that may be forgotten or bypassed. Entities should consider requiring security awareness training anytime personnel transfer into roles where they can impact the security of cardholder data and/or sensitive authentication data from roles where they did not have this impact. Methods and training content can vary, depending on personnel roles. **Examples** Different methods that can be used to provide security awareness and education include posters, letters, web-based training, in-person training, team meetings, and incentives. Personnel acknowledgments may be recorded in writing or electronically.
12.6.3 Personnel receive security awareness training as follows: • Upon hire and at least once every 12 months. • Multiple methods of communication are used. • Personnel acknowledge at least once every 12 months that they have read and understood the information security policy and procedures.	**12.6.3.a** Examine security awareness program records to verify that personnel attend security awareness training upon hire and at least once every 12 months. **12.6.3.b** Examine security awareness program materials to verify the program includes multiple methods of communicating awareness and educating personnel.	
	12.6.3.c Interview personnel to verify they have completed awareness training and are aware of their role in protecting cardholder data.	
Customized Approach Objective	**12.6.3.d** Examine security awareness program materials and personnel acknowledgments to verify that personnel acknowledge at least once every 12 months that they have read and understand the information security policy and procedures.	
Personnel remain knowledgeable about the threat landscape, their responsibility for the operation of relevant security controls, and are able to access assistance and guidance when required.		

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Educating personnel on how to detect, react to, and report potential phishing and related attacks and social engineering attempts is essential to minimizing the probability of successful attacks. **Good Practice** An effective security awareness program should include examples of phishing emails and periodic testing to determine the prevalence of personnel reporting such attacks. Training material an entity can consider for this topic include: • How to identify phishing and other social engineering attacks. • How to react to suspected phishing and social engineering. • Where and how to report suspected phishing and social engineering activity. An emphasis on reporting allows the organization to reward positive behavior, to optimize technical defenses (see Requirement 5.4.1), and to take immediate action to remove similar phishing emails that evaded technical defenses from recipient inboxes.
12.6.3.1 Security awareness training includes awareness of threats and vulnerabilities that could impact the security of cardholder data and/or sensitive authentication data, including but not limited to: • Phishing and related attacks. • Social engineering.	**12.6.3.1** Examine security awareness training content to verify it includes all elements specified in this requirement.	
Customized Approach Objective		
Personnel are knowledgeable about their own human vulnerabilities and how threat actors will attempt to exploit such vulnerabilities. Personnel are able to access assistance and guidance when required.		
Applicability Notes		
See Requirement 5.4.1 for guidance on the difference between technical and automated controls to detect and protect users from phishing attacks, and this requirement for providing users security awareness training about phishing and social engineering. These are two separate and distinct requirements, and one is not met by implementing controls required by the other one. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** By including the key points of the acceptable use policy in regular training and the related context, personnel will understand their responsibilities and how these impact the security of an organization's systems.
12.6.3.2 Security awareness training includes awareness about the acceptable use of end-user technologies in accordance with Requirement 12.2.1.	**12.6.3.2** Examine security awareness training content to verify it includes awareness about acceptable use of end-user technologies in accordance with Requirement 12.2.1.	
Customized Approach Objective		
Personnel are knowledgeable about their responsibility for the security and operation of end-user technologies and are able to access assistance and guidance when required.		
Applicability Notes		
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.		

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
12.7 Personnel are screened to reduce risks from insider threats.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Performing thorough screening prior to hiring potential personnel who are expected to be given access to the CDE provides entities with the information necessary to make informed risk decisions regarding personnel they hire that will have access to the CDE. Other benefits of screening potential personnel include helping to ensure workplace safety and confirming information provided by prospective employees on their resumes. **Good Practice** Entities should consider screening for existing personnel anytime they transfer into roles where they have access to the CDE from roles where they did not have this access. To be effective, the level of screening should be appropriate for the position. For example, positions requiring greater responsibility or that have administrative access to critical data or systems may warrant more detailed or more frequent screening than positions with less responsibility and access. **Examples** Screening options can include, as appropriate for the entity's region, previous employment history, review of public information/social media resources, criminal record, credit history, and reference checks.
12.7.1 Potential personnel who will have access to the CDE are screened, within the constraints of local laws, prior to hire to minimize the risk of attacks from internal sources.	**12.7.1** Interview responsible Human Resource department management to verify that screening is conducted, within the constraints of local laws, prior to hiring potential personnel who will have access to the CDE.	
Customized Approach Objective		
The risk related to allowing new members of staff access to the CDE is understood and managed.		
Applicability Notes		
For those potential personnel to be hired for positions such as store cashiers, who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.		

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Maintaining a list of all TPSPs identifies where potential risk extends outside the organization and defines the organization's extended attack surface. **Examples** Different types of TPSPs include those that: • Store, process, or transmit account data on the entity's behalf (such as payment gateways, payment processors, payment service providers (PSPs), and off-site storage providers). • Manage system components included in the entity's PCI DSS assessment (such as providers of network security control services, anti-malware services, and security incident and event management (SIEM); contact and call centers; web-hosting companies; and IaaS, PaaS, SaaS, and FaaS cloud providers). • Could impact the security of the entity's cardholder data and/or sensitive authentication data (such as vendors providing support via remote access, and bespoke software developers).
12.8.1 A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.	**12.8.1.a** Examine policies and procedures to verify that processes are defined to maintain a list of TPSPs, including a description for each of the services provided, for all TPSPs with whom account data is shared or that could affect the security of account data.	
	12.8.1.b Examine documentation to verify that a list of all TPSPs is maintained that includes a description of the services provided.	
Customized Approach Objective		
Records are maintained of TPSPs and the services provided.		
Applicability Notes		
The use of a PCI DSS compliant TPSP does not make an entity PCI DSS compliant, nor does it remove the entity's responsibility for its own PCI DSS compliance.		

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** The written acknowledgment from a TPSP demonstrates its commitment to maintaining proper security of account data that it obtains from its customers and that the TPSP is fully aware of the assets that could be affected during the provisioning of the TPSP's service. The extent to which a specific TPSP is responsible for the security of account data will depend on the service provided and the responsibilities agreed between the provider and assessed entity (the customer). In conjunction with Requirement 12.9.1, this requirement is intended to promote a consistent level of understanding between parties about their applicable PCI DSS responsibilities. For example, the agreement may include the applicable PCI DSS requirements to be maintained as part of the provided service.
12.8.2 Written agreements with TPSPs are maintained as follows: • Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE. • Written agreements include acknowledgments from TPSPs that TPSPs are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that the TPSP could impact the security of the entity's cardholder data and/or sensitive authentication data.	**12.8.2.a** Examine policies and procedures to verify that processes are defined to maintain written agreements with all TPSPs in accordance with all elements specified in this requirement. **12.8.2.b** Examine written agreements with TPSPs to verify they are maintained in accordance with all elements as specified in this requirement.	
Customized Approach Objective		
Records are maintained of each TPSP's acknowledgment of its responsibility to protect account data.		

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
Applicability Notes The exact wording of an agreement will depend on the details of the service being provided, and the responsibilities assigned to each party. The agreement does not have to include the exact wording provided in this requirement. The TPSP's written acknowledgment is a confirmation that states the TPSP is responsible for the security of the account data it may store, process, or transmit on behalf of the customer or to the extent the TPSP may impact the security of a customer's cardholder data and/or sensitive authentication data. Evidence that a TPSP is meeting PCI DSS requirements (is not the same as a written acknowledgment specified in this requirement. For example, a PCI DSS Attestation of Compliance (AOC), a declaration on a company's website, a policy statement, a responsibility matrix, or other evidence not included in a written agreement is not a written acknowledgment.		**Good Practice** The entity may also want to consider including in their written agreement with a TPSP that the TPSP will support the entity's request for information per Requirement 12.9.2. Entities will also want to understand whether any TPSPs have "nested" relationships with other TPSPs, meaning the primary TPSP contracts with another TPSP(s) for the purposes of providing a service. It is important to understand whether the primary TPSP is relying on the secondary TPSP(s) to achieve overall compliance of a service, and what types of written agreements the primary TPSP has in place with the secondary TPSPs. Entities can consider including coverage in their written agreement for any "nested" TPSPs a primary TPSP may use. **Further Information** Refer to the *Information Supplement: Third-Party Security Assurance* for further guidance.

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** A thorough process for engaging TPSPs, including details for selection and vetting prior to engagement, helps ensure that a TPSP is thoroughly vetted internally by an entity prior to establishing a formal relationship and that the risk to cardholder data associated with the engagement of the TPSP is understood. **Good Practice** Specific due-diligence processes and goals will vary for each organization. Elements that should be considered include the provider's reporting practices, breach-notification and incident response procedures, details of how PCI DSS responsibilities are assigned between each party, how the TPSP validates their PCI DSS compliance and what evidence they provide.
12.8.3 An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement.	**12.8.3.a** Examine policies and procedures to verify that processes are defined for engaging TPSPs, including proper due diligence prior to engagement.	
	12.8.3.b Examine evidence and interview responsible personnel to verify the process for engaging TPSPs includes proper due diligence prior to engagement.	
Customized Approach Objective		
The capability, intent, and resources of a prospective TPSP to adequately protect account data are assessed before the TPSP is engaged.		

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Knowing the PCI DSS compliance status of all engaged TPSPs provides assurance and awareness about whether they comply with the requirements applicable to the services they offer to the organization. **Good Practice** If the TPSP offers a variety of services, the compliance status the entity monitors should be specific to those services delivered to the entity and those services in scope for the entity's PCI DSS assessment. *(continued on next page)*
12.8.4 A program is implemented to monitor TPSPs' PCI DSS compliance status at least once every 12 months.	**12.8.4.a** Examine policies and procedures to verify that processes are defined to monitor TPSPs' PCI DSS compliance status at least once every 12 months.	
	12.8.4.b Examine documentation and interview responsible personnel to verify that the PCI DSS compliance status of each TPSP is monitored at least once every 12 months.	
Customized Approach Objective		
The PCI DSS compliance status of TPSPs is verified periodically.		

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
Applicability Notes Where an entity has an agreement with a TPSP for meeting PCI DSS requirements on behalf of the entity (for example, via a firewall service), the entity must work with the TPSP to make sure the applicable PCI DSS requirements are met. If the TPSP does not meet those applicable PCI DSS requirements, then those requirements are also "not in place" for the entity.		If a TPSP has a PCI DSS Attestation of Compliance (AOC), the expectation is that the TPSP should provide that to customers upon request to demonstrate their PCI DSS compliance status. If the TPSP did not undergo a PCI DSS assessment, it may be able to provide other sufficient evidence to demonstrate that it has met the applicable requirements without undergoing a formal compliance validation. For example, the TPSP can provide specific evidence to the entity's assessor so the assessor can confirm applicable requirements are met. Alternatively, the TPSP can elect to undergo multiple on-demand assessments by each of its customers' assessors, with each assessment targeted to confirm that applicable requirements are met. **Further Information** For more information about third-party service providers, refer to: • PCI DSS section: Use of Third-Party Service Providers. • *Information Supplement: Third-Party Security Assurance*.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** It is important that the entity understands which PCI DSS requirements and sub-requirements its TPSPs have agreed to meet, which requirements are shared between the TPSP and the entity, and for those that are shared, specifics about how the requirements are shared and which entity is responsible for meeting each sub-requirement. Without this shared understanding, it is inevitable that the entity and the TPSP will assume a given PCI DSS sub-requirement is the responsibility of the other party, and therefore that sub-requirement may not be addressed at all. The specific information an entity maintains will depend on the particular agreement with their providers, the type of service, etc. TPSPs may define their PCI DSS responsibilities to be the same for all their customers; otherwise, this responsibility should be agreed upon by both the entity and TPSP. **Good Practice** Entities can document these responsibilities via a matrix that identifies all applicable PCI DSS requirements and indicates for each requirement whether the entity or TPSP is responsible for meeting that requirement or whether it is a shared responsibility. This type of document is often referred to as a *responsibility matrix*. *(continued on next page)*
12.8.5 Information is maintained about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between the TPSP and the entity.	**12.8.5.a** Examine policies and procedures to verify that processes are defined to maintain information about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between both the TPSP and the entity.	
	12.8.5.b Examine documentation and interview personnel to verify the entity maintains information about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between both entities.	
Customized Approach Objective		
Records detailing the PCI DSS requirements and related system components for which each TPSP is solely or jointly responsible, are maintained and reviewed periodically.		

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
12.8.5 *(continued)*		It is also important for entities to understand whether any TPSPs have "nested" relationships with other TPSPs, meaning the primary TPSP contracts with another TPSP(s) for the purposes of providing a service. It is important to understand whether the primary TPSP is relying on the secondary TPSP(s) to achieve overall compliance of a service, and how the primary TPSP is monitoring performance of the service and the PCI DSS compliance status of the secondary TPSP(s). Note that it is the responsibility of the primary TPSP to manage and monitor any secondary TPSPs. **Further Information** Refer to *Information Supplement: Third-Party Security Assurance* for a sample responsibility matrix template.

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
12.9 Third-party service providers (TPSPs) support their customers' PCI DSS compliance.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** In conjunction with Requirement 12.8.2, this requirement is intended to promote a consistent level of understanding between TPSPs and their customers about their applicable PCI DSS responsibilities. The acknowledgment from the TPSP evidences the TPSP's commitment to maintaining proper security of the account data that it obtains from its customers. The TPSP's internal policies and procedures related to their customer engagement process and any templates used for written agreements should include provision of an applicable PCI DSS acknowledgement to its customers. The method by which the TPSP provides written acknowledgment should be agreed between the provider and its customers.
12.9.1 *Additional requirement for service providers only:* TPSPs provide written agreements to customers that include acknowledgments that TPSPs are responsible for the security of account data the TPSP possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that the TPSP could impact the security of the customer's cardholder data and/or sensitive authentication data.	**12.9.1 *Additional testing procedure for service provider assessments only:*** Examine TPSP policies, procedures, and templates used for written agreements to verify processes are defined for the TPSP to provide written acknowledgments to customers in accordance with all elements specified in this requirement.	
Customized Approach Objective		
TPSPs formally acknowledge their security responsibilities to their customers. *(continued on next page)*		

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
Applicability Notes This requirement applies only when the entity being assessed is a service provider. The exact wording of an agreement will depend on the details of the service being provided, and the responsibilities assigned to each party. The agreement does not have to include the exact wording provided in this requirement. The TPSP's written acknowledgment is a confirmation that states the TPSP is responsible for the security of the account data it may store, process, or transmit on behalf of the customer or to the extent the TPSP may impact the security of a customer's cardholder data and/or sensitive authentication data. Evidence that a TPSP is meeting PCI DSS requirements is not the same as a written agreement specified in this requirement. For example, a PCI DSS Attestation of Compliance (AOC), a declaration on a company's website, a policy statement, a responsibility matrix, or other evidence not included in a written agreement is not a written acknowledgment.		

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If a TPSP does not provide the necessary information to enable its customers to meet their security and compliance requirements, the customers will not be able to protect cardholder data nor meet their own contractual obligations. **Good Practice** If a TPSP has a PCI DSS Attestation of Compliance (AOC), the expectation is that the TPSP should provide that to customers upon request to demonstrate their PCI DSS compliance status. If the TPSP did not undergo a PCI DSS assessment, they may be able to provide other sufficient evidence to demonstrate that it has met the applicable requirements without undergoing a formal compliance validation. For example, the TPSP can provide specific evidence to the entity's assessor so the assessor can confirm applicable requirements are met. Alternatively, the TPSP can elect to undergo multiple on-demand assessments by each of its customers' assessors, with each assessment targeted to confirm that applicable requirements are met. TPSPs should provide sufficient evidence to their customers to verify that the scope of the TPSP's PCI DSS assessment covered the services applicable to the customer and that the relevant PCI DSS requirements were examined and determined to be in place. *(continued on next page)*
12.9.2 ***Additional requirement for service providers only:*** TPSPs support their customers' requests for information to meet Requirements 12.8.4 and 12.8.5 by providing the following upon customer request: • PCI DSS compliance status information (Requirement 12.8.4). • Information about which PCI DSS requirements are the responsibility of the TPSP and which are the responsibility of the customer, including any shared responsibilities (Requirement 12.8.5), for any service the TPSP provides that meets a PCI DSS requirement(s) on behalf of customers or that can impact security of customers' cardholder data or sensitive authentication data.	**12.9.2** ***Additional testing procedure for service provider assessments only:*** Examine policies and procedures to verify processes are defined for the TPSPs to support customers' request for information to meet Requirements 12.8.4 and 12.8.5 in accordance with all elements specified in this requirement.	
Customized Approach Objective		
TPSPs provide information as needed to support their customers' PCI DSS compliance efforts.		
Applicability Notes		
This requirement applies only when the entity being assessed is a service provider.		

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
12.9.2 *(continued)*		TPSPs may define their PCI DSS responsibilities to be the same for all their customers; otherwise, this responsibility should be agreed upon by both the customer and TPSP. It is important that the customer understands which PCI DSS requirements and sub-requirements its TPSPs have agreed to meet, which requirements are shared between the TPSP and the customer, and for those that are shared, specifics about how the requirements are shared and which entity is responsible for meeting each sub-requirement. An example of a way to document these responsibilities is via a matrix that identifies all applicable PCI DSS requirements and indicates whether the customer or TPSP is responsible for meeting that requirement or whether it is a shared responsibility. **Further Information** For further guidance, refer to: • PCI DSS section: *Use of Third-Party Service Providers*. • *Information Supplement: Third-Party Security Assurance* (includes a sample responsibility matrix template).

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Without a comprehensive incident response plan that is properly disseminated, read, and understood by the parties responsible, confusion and lack of a unified response could create further downtime for the business, unnecessary public media exposure, as well as risk of financial and/or reputational loss and legal liabilities. **Good Practice** The incident response plan should be thorough and contain all the key elements for stakeholders (for example, legal, communications) to allow the entity to respond effectively in the event of a breach that could impact account data. It is important to keep the plan up to date with current contact information of all individuals designated as having a role in incident response. Other relevant parties for notifications may include customers, financial institutions (acquirers and issuers), and business partners. Entities should consider how to address all compromises of data within the CDE in their incident response plans, including compromises to account data, wireless encryption keys, encryption keys used for transmission and storage or account data or cardholder data, etc. *(continued on next page)*
12.10.1 An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to: • Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum. • Incident response procedures with specific containment and mitigation activities for different types of incidents. • Business recovery and continuity procedures. • Data backup processes. • Analysis of legal requirements for reporting compromises. • Coverage and responses of all critical system components. • Reference or inclusion of incident response procedures from the payment brands.	**12.10.1.a** Examine the incident response plan to verify that the plan exists and includes at least the elements specified in this requirement.	
	12.10.1.b Interview personnel and examine documentation from previously reported incidents or alerts to verify that the documented incident response plan and procedures were followed.	
Customized Approach Objective		
A comprehensive incident response plan that meets card brand expectations is maintained.		

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
12.10.1 *(continued)*		**Examples** Legal requirements for reporting compromises include those in most US states, the EU General Data Protection Regulation (GDPR), and the Personal Data Protection Act (Singapore). **Further Information** For more information, refer to the *NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide*.
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Proper testing of the security incident response plan can identify broken business processes and ensure key steps are not missed, which could result in increased exposure during an incident. Periodic testing of the plan ensures that the processes remain viable, as well as ensuring that all relevant personnel in the organization are familiar with the plan. **Good Practice** The test of the incident response plan can include simulated incidents and the corresponding responses in the form of a “table-top exercise” that includes participation by relevant personnel. A review of the incident and the quality of the response can provide entities with the assurance that all required elements are included in the plan.
12.10.2 At least once every 12 months, the security incident response plan is: • Reviewed and the content is updated as needed. • Tested, including all elements listed in Requirement 12.10.1.	**12.10.2** Interview personnel and review documentation to verify that, at least once every 12 months, the security incident response plan is: • Reviewed and updated as needed. • Tested, including all elements listed in Requirement 12.10.1.	
Customized Approach Objective		
The incident response plan is kept current and tested periodically.		

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** An incident could occur at any time, therefore if a person who is trained in incident response and familiar with the entity's plan is available when an incident is detected, the entity's ability to correctly respond to the incident is increased. **Good Practice** Often, specific personnel are designated to be part of a security incident response team, with the team having overall responsibility for responding to incidents (perhaps on a rotating schedule basis) and managing those incidents in accordance with the plan. The incident response team can consist of core members who are permanently assigned or "on-demand" personnel who may be called up as necessary, depending on their expertise and the specifics of the incident. Having available resources to respond quickly to incidents minimizes disruption to the organization. Examples of types of activity the team or individuals should respond to include any evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and reports of unauthorized critical system or content file changes.
12.10.3 Specific personnel are designated to be available on a 24/7 basis to respond to suspected or confirmed security incidents.	**12.10.3** Examine documentation and interview responsible personnel occupying designated roles to verify that specific personnel are designated to be available on a 24/7 basis to respond to security incidents.	
Customized Approach Objective		
Incidents are responded to immediately where appropriate.		

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	
12.10.4 Personnel responsible for responding to suspected and confirmed security incidents are appropriately and periodically trained on their incident response responsibilities. **Customized Approach Objective** Personnel are knowledgeable about their role and responsibilities in incident response and are able to access assistance and guidance when required.	**12.10.4** Examine training documentation and interview incident response personnel to verify that personnel are appropriately and periodically trained on their incident response responsibilities.	**Purpose** Without a trained and readily available incident response team, extended damage to the network could occur, and critical data and systems may become "polluted" by inappropriate handling of the targeted systems. This can hinder the success of a post-incident investigation. **Good Practice** It is important that all personnel involved in incident response are trained and knowledgeable about managing evidence for forensics and investigations.
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Each entity's environment and incident response plan are different, and the approach will depend on a number of factors, including the size and complexity of the entity, the degree of change in the environment, the size of the incident response team, and the turnover in personnel. Performing a risk analysis will allow the entity to determine the optimum frequency for training personnel with incident response responsibilities.
12.10.4.1 The frequency of periodic training for incident response personnel is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.	**12.10.4.1.a** Examine the entity's targeted risk analysis for the frequency of training for incident response personnel to verify the risk analysis was performed in accordance with all elements specified in Requirement 12.3.1.	
Customized Approach Objective Incident response personnel are trained at a frequency that addresses the entity's risk. **Applicability Notes** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	**12.10.4.1.b** Examine documented results of periodic training of incident response personnel and interview personnel to verify training is performed at the frequency defined in the entity's targeted risk analysis performed for this requirement.	

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Responding to alerts generated by security monitoring systems that are explicitly designed to focus on potential risk to data is critical to prevent a breach and therefore, this must be included in the incident-response processes.
12.10.5 The security incident response plan includes monitoring and responding to alerts from security monitoring systems, including but not limited to: • Intrusion-detection and intrusion-prevention systems. • Network security controls. • Change-detection mechanisms for critical files. • The change-and tamper-detection mechanism for payment pages. *This bullet is a best practice until its effective date; refer to Applicability Notes below for details.* • Detection of unauthorized wireless access points.	**12.10.5** Examine documentation and observe incident response processes to verify that monitoring and responding to alerts from security monitoring systems are covered in the security incident response plan, including but not limited to the systems specified in this requirement.	
Customized Approach Objective		
Alerts generated by monitoring and detection technologies are responded to in a structured, repeatable manner.		
Applicability Notes		
The bullet above (for monitoring and responding to alerts from a change- and tamper-detection mechanism for payment pages) is a best practice until 31 March 2025, after which it will be required as part of Requirement 12.10.5 and must be fully considered during a PCI DSS assessment.		

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Incorporating lessons learned into the incident response plan after an incident occurs and in-step with industry developments, helps keep the plan current and able to react to emerging threats and security trends. **Good Practice** The lessons-learned exercise should include all levels of personnel. Although it is often included as part of the review of the entire incident, it should focus on how the entity's response to the incident could be improved. It is important to not just consider elements of the response that did not have the planned outcomes but also to understand what worked well and whether lessons from those elements that worked well can be applied to areas of the plan that did not. Another way to optimize an entity's incident response plan is to understand the attacks made against other organizations and use that information to fine-tune the entity's detection, containment, mitigation, or recovery procedures.
12.10.6 The security incident response plan is modified and evolved according to lessons learned and to incorporate industry developments.	**12.10.6.a** Examine policies and procedures to verify that processes are defined to modify and evolve the security incident response plan according to lessons learned and to incorporate industry developments.	
	12.10.6.b Examine the security incident response plan and interview responsible personnel to verify that the incident response plan is modified and evolved according to lessons learned and to incorporate industry developments.	
Customized Approach Objective		
The effectiveness and accuracy of the incident response plan is reviewed and updated after each invocation.		

Exhibit 22A-12

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	
12.10.7 Incident response procedures are in place, to be initiated upon the detection of stored PAN anywhere it is not expected, and include: • Determining what to do if PAN is discovered outside the CDE, including its retrieval, secure deletion, and/or migration into the currently defined CDE, as applicable. • Identifying whether sensitive authentication data is stored with PAN. • Determining where the account data came from and how it ended up where it was not expected. • Remediating data leaks or process gaps that resulted in the account data being where it was not expected.	**12.10.7.a** Examine documented incident response procedures to verify that procedures for responding to the detection of stored PAN anywhere it is not expected to exist, ready to be initiated, and include all elements specified in this requirement. **12.10.7.b** Interview personnel and examine records of response actions to verify that incident response procedures are performed upon detection of stored PAN anywhere it is not expected.	**Purpose** Having documented incident response procedures that are followed in the event that stored PAN is found anywhere it is not expected to be, helps to identify the necessary remediation actions and prevent future leaks. **Good Practice** If PAN was found outside the CDE, analysis should be performed to 1) determine whether it was saved independently of other data or with sensitive authentication data, 2) identify the source of the data, and 3) identify the control gaps that resulted in the data being outside the CDE. Entities should consider whether there are contributory factors, such as business processes, user behavior, improper system configurations, etc. that caused the PAN to be stored in an unexpected location. If such contributory factors are present, they should be addressed per this Requirement to prevent recurrence.
Customized Approach Objective		
Processes are in place to quickly respond, analyze, and address situations in the event that cleartext PAN is detected where it is not expected.		
Applicability Notes		
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.		

Exhibit 22A-13

4 Scope of PCI DSS Requirements

PCI DSS requirements apply to:

- The cardholder data environment (CDE), which is comprised of:
  - System components, people, and processes that store, process, or transmit cardholder data and/or sensitive authentication data, and,
  - System components that may not store, process, or transmit CHD/SAD but have unrestricted connectivity to system components that store, process, or transmit CHD/SAD.

AND

- System components, people, and processes that could impact the security of cardholder data and/or sensitive authentication data. [4]

"System components" include network devices, servers, computing devices, virtual components, cloud components, and software. Examples of system components include but are not limited to:

- Systems that store, process, or transmit account data (for example, payment terminals, authorization systems, clearing systems, payment middleware systems, payment back-office systems, shopping cart and store front systems, payment gateway/switch systems, fraud monitoring systems).
- Systems that provide security services (for example, authentication servers, access control servers, security information and event management (SIEM) systems, physical security systems (for example, badge access or CCTV), multi-factor authentication systems, anti-malware systems).
- Systems that facilitate segmentation (for example, internal network security controls).
- Systems that could impact the security of account data or the CDE (for example, name resolution, or e-commerce (web) redirection servers).
- Virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors.
- Cloud infrastructure and components, both external and on premises, and including instantiations of containers or images, virtual private clouds, cloud-based identity and access management, CDEs residing on premises or in the cloud, service meshes with containerized applications, and container orchestration tools.

[4] For additional guidance, refer to *Information Supplement: Guidance for PCI DSS Scoping and Network Segmentation* on the PCI SSC website.

Exhibit 22A-13

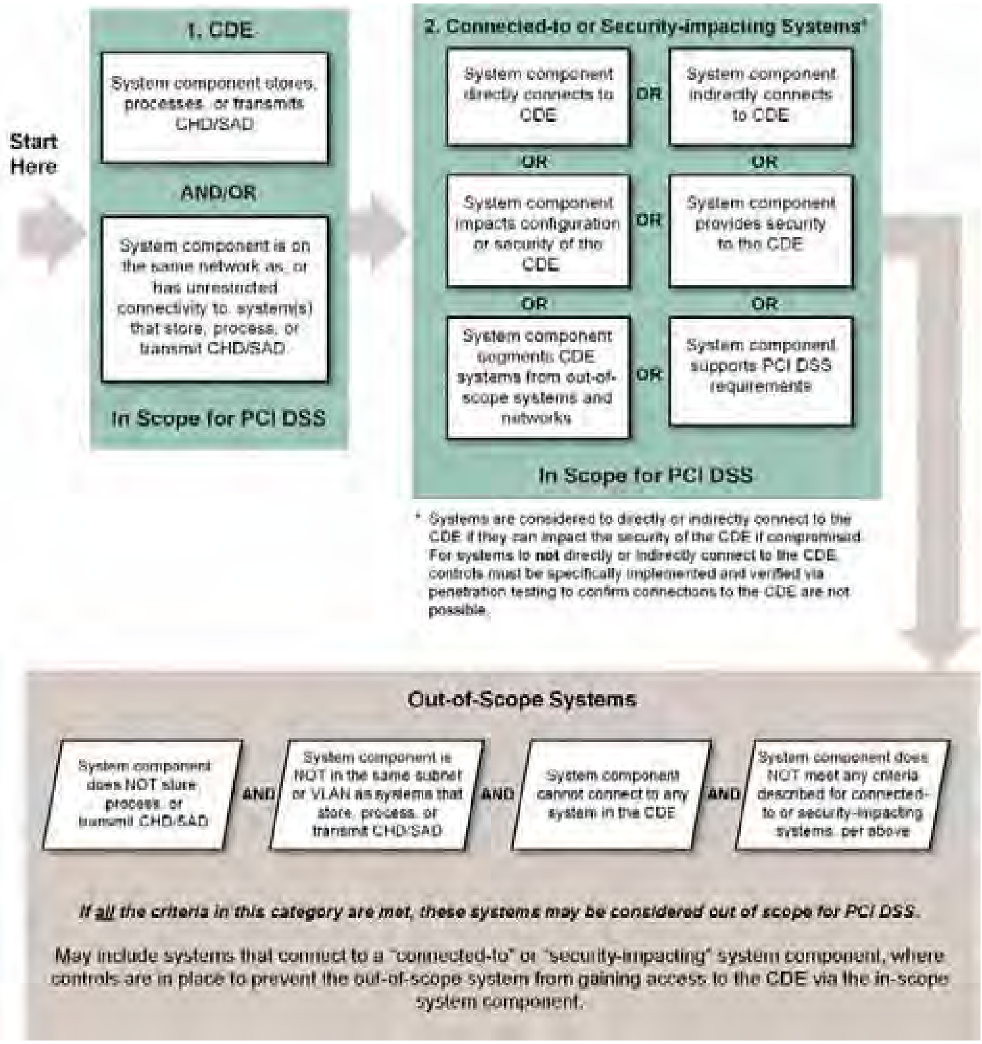
- Network components, including but not limited to network security controls, switches, routers, VoIP network devices, wireless access points, network appliances, and other security appliances.
- Server types, including but not limited to web, application, database, authentication, mail, proxy, Network Time Protocol (NTP), and Domain Name System (DNS).
- End-user devices, such as computers, laptops, workstations, administrative workstations, tablets, and mobile devices.
- Printers, and multi-function devices that scan, print, and fax.
- Storage of account data in any format (for example, paper, data files, audio files, images, and video recordings).
- Applications, software, and software components, serverless applications, including all purchased, subscribed (for example, Software-as-a-Service), bespoke and custom software, including internal and external (for example, Internet) applications.
- Tools, code repositories, and systems that implement software configuration management or for deployment of objects to the CDE or to systems that can impact the CDE.

2 of 3

Exhibit 22A-13

Figure 1 shows considerations for scoping system components for PCI DSS.

Figure 1. Understanding PCI DSS Scoping


Start Here
1. CDE
System component stores, processes, or transmits CHD/SAD
AND/OR
System component is on the same network as, or has unrestricted connectivity to, system(s) that store, process, or transmit CHD/SAD
In Scope for PCI DSS
2. Connected-to or Security-impacting Systems*
System component directly connects to CDE
OR
System component indirectly connects to CDE
OR
OR
System component impacts configuration or security of the CDE
OR
System component provides security to the CDE
OR
OR
System component segments CDE systems from out-of-scope systems and networks
OR
System component supports PCI DSS requirements
In Scope for PCI DSS
Out-of-Scope Systems
System component does NOT store, process, or transmit CHD/SAD
AND
System component is NOT in the same subnet or VLAN as systems that store, process, or transmit CHD/SAD
AND
System component cannot connect to any system in the CDE
AND
System component does NOT meet any criteria described for connected-to or security-impacting systems, per above

* Systems are considered to directly or indirectly connect to the CDE if they can impact the security of the CDE if compromised. For systems to **not** directly or indirectly connect to the CDE, controls must be specifically implemented and verified via penetration testing to confirm connections to the CDE are not possible.

If all the criteria in this category are met, these systems may be considered out of scope for PCI DSS.

May include systems that connect to a "connected-to" or "security-impacting" system component, where controls are in place to prevent the out-of-scope system from gaining access to the CDE via the in-scope system component.

Exhibit 22A-14

1 Introduction and PCI Data Security Standard Overview

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance payment account data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data. While specifically designed to focus on environments with payment account data, PCI DSS can also be used to protect against threats and secure other elements in the payment ecosystem.

Table 1 shows the 12 principal PCI DSS requirements.

Table 1. Principal PCI DSS Requirements

PCI Data Security Standard – High Level Overview	
Build and Maintain a Secure Network and Systems	**1.** Install and Maintain Network Security Controls. **2.** Apply Secure Configurations to All System Components.
Protect Account Data	**3.** Protect Stored Account Data. **4.** Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks.
Maintain a Vulnerability Management Program	**5.** Protect All Systems and Networks from Malicious Software. **6.** Develop and Maintain Secure Systems and Software.
Implement Strong Access Control Measures	**7.** Restrict Access to System Components and Cardholder Data by Business Need to Know. **8.** Identify Users and Authenticate Access to System Components. **9.** Restrict Physical Access to Cardholder Data.
Regularly Monitor and Test Networks	**10.** Log and Monitor All Access to System Components and Cardholder Data. **11.** Test Security of Systems and Networks Regularly.
Maintain an Information Security Policy	**12.** Support Information Security with Organizational Policies and Programs.

This document, the Payment Card Industry Data Security Standard Requirements and Testing Procedures, consists of the 12 PCI DSS principal requirements, detailed security requirements, corresponding testing procedures, and other information pertinent to each requirement. The following sections provide detailed guidelines and best practices to assist entities to prepare for, conduct, and report the results of a PCI DSS assessment. The PCI DSS requirements and testing procedures begin on page 43.

Exhibit 22A-14

PCI DSS comprises a minimum set of requirements for protecting account data and may be enhanced by additional controls and practices to further mitigate risks, and to incorporate local, regional, and sector laws and regulations. Additionally, legislation or regulatory requirements may require specific protection of personal information or other data elements (for example, cardholder name).

Limitations

If any of the requirements contained in this standard conflict with country, state, or local laws, the country, state, or local law will apply.

PCI DSS Resources

The PCI Security Standards Council (PCI SSC) website (www.pcisecuritystandards.org) provides the following additional resources to assist organizations with their PCI DSS assessments and validations:

- Document Library, including:
  - PCI DSS Summary of Changes
  - PCI DSS Quick Reference Guide
  - Information Supplements and Guidelines
  - Prioritized Approach for PCI DSS
  - Report on Compliance (ROC) Reporting Template and Reporting Instructions
  - Self-Assessment Questionnaires (SAQs) and SAQ Instructions and Guidelines
  - Attestations of Compliance *(AOCs)*
- Frequently Asked Questions (FAQs)
- PCI for Small Merchants website
- PCI training courses and informational webinars
- List of Qualified Security Assessors (QSAs) and Approved Scanning Vendors (ASVs)
- Lists of PCI approved devices, applications, and solutions

Exhibit 22A-14

There are over 60 guidance documents and information supplements available on the PCI SSC website that provide specific guidance and considerations for PCI DSS. Examples include:

- Guidance for PCI DSS Scoping and Network Segmentation
- PCI SSC Cloud Computing Guidelines
- Multi-Factor Authentication Guidance
- Third-Party Security Assurance
- Effective Daily Log Monitoring
- Penetration Testing Guidance
- Best Practices for Implementing a Security Awareness Program
- Best Practices for Maintaining PCI DSS Compliance
- PCI DSS for Large Organizations
- Use of SSL/Early TLS and Impact on ASV Scans
- Use of SSL/Early TLS for POS POI Terminal Connections
- Tokenization Product Security Guidelines
- Protecting Telephone-Based Payment Card Data

Note: *Information Supplements complement PCI DSS and identify additional considerations and recommendations for meeting PCI DSS requirements. Information Supplements do not supersede, replace, or extend PCI DSS or any of its requirements.*

Refer to the Document Library at www.pcisecuritystandards.org for information about these and other resources.

In addition, refer to *Appendix G* for definitions of PCI DSS terms.

3 of 3

Exhibit 22A-15

Appendix G PCI DSS Glossary of Terms, Abbreviations, and Acronyms

Term	Definition
Account	Also referred to as “user ID,” “account ID,” or “application ID.” Used to identify an individual or process on a computer system. See *Authentication Credentials* and *Authentication Factor*.
Account Data	Account data consists of cardholder data and/or sensitive authentication data. See *Cardholder Data* and *Sensitive Authentication Data*.
Acquirer	Also referred to as “merchant bank,” “acquiring bank,” or “acquiring financial institution.” Entity, typically a financial institution, that processes payment card transactions for merchants and is defined by a payment brand as an acquirer. Acquirers are subject to payment brand rules and procedures regarding merchant compliance. See *Payment Processor*.
Administrative Access	Elevated or increased privileges granted to an account for that account to manage systems, networks, and/or applications. Administrative access can be assigned to an individual’s account or a built-in system account. Accounts with administrative access are often referred to as “superuser,” “root,” “administrator,” “admin,” “sysadmin,” or “supervisor-state,” depending on the particular operating system and organizational structure.
AES	Acronym for “Advanced Encryption Standard.” See *Strong Cryptography.*
ANSI	Acronym for “American National Standards Institute.”
Anti-Malware	Software that is designed to detect, and remove, block, or contain various forms of malicious software.
AOC	Acronym for “Attestation of Compliance.” The AOC is the official PCI SSC form for merchants and service providers to attest to the results of a PCI DSS assessment, as documented in a Self-Assessment Questionnaire (SAQ) or Report on Compliance (ROC).
Application	Includes all purchased, custom, and bespoke software programs or groups of programs, including both internal and external (for example, web) applications.
Application and System Accounts	Also referred to as “service accounts.” Accounts that execute processes or perform tasks on a computer system or in an application. These accounts usually have elevated privileges that are required to perform specialized tasks or functions and are not typically accounts used by an individual.
ASV	Acronym for “Approved Scanning Vendor.” Company approved by the PCI SSC to conduct external vulnerability scanning services.

Exhibit 22A-15

Term	Definition
Audit Log	Also referred to as "audit trail." Chronological record of system activities. Provides an independently verifiable trail sufficient to permit reconstruction, review, and examination of sequence of environments and activities surrounding or leading to operation, procedure, or event in a transaction from inception to final results.
Authentication	Process of verifying identity of an individual, device, or process. Authentication typically occurs with one or more authentication factors. See *Account, Authentication Credential,* and *Authentication Factor.*
Authentication Credential	Combination of the user ID or account ID plus the authentication factor(s) used to authenticate an individual, device, or process. See *Account* and *Authentication Factor.*
Authentication Factor	The element used to prove or verify the identity of an individual or process on a computer system. Authentication typically occurs with one or more of the following authentication factors: • Something you know, such as a password or passphrase, • Something you have, such as a token device or smart card, • Something you are, such as a biometric element. The ID (or account) and authentication factor together are considered authentication credentials. See *Account* and *Authentication Credential.*
Authorization	In the context of access control, authorization is the granting of access or other rights to a user, program, or process. Authorization defines what an individual or program can do after successful authentication. In the context of a payment card transaction, authorization refers to the authorization process, which completes when a merchant receives a transaction response (for example, an approval or decline).
BAU	Acronym for "Business as Usual."
Bespoke and Custom Software	*Bespoke software* is developed for the entity by a third party on the entity's behalf and per the entity's specifications. *Custom software* is developed by the entity for its own use.
Card Skimmer	A physical device, often attached to a legitimate card-reading device, designed to illegitimately capture and/or store the information from a payment card.
Card Verification Code	Also referred to as Card Validation Code or Value, or Card Security Code. For PCI DSS purposes, it is the three- or four-digit value printed on the front or back of a payment card. May be referred to as CAV2, CVC2, CVN2, CVV2, or CID according to the individual Participating Payment Brands. For more information, contact the Participating Payment Brands.

Exhibit 22A-15

Term	Definition
Cardholder	Customer to which a payment card is issued, or any individual authorized to use the payment card. See *Visitor.*
Cardholder Data (CHD)	At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code. See *Sensitive Authentication Data* for additional data elements that might be transmitted or processed (but not stored) as part of a payment transaction.
CDE	Acronym for “Cardholder Data Environment.” The CDE is comprised of: • The system components, people, and processes that store, process, or transmit cardholder data and/or sensitive authentication data, and, • System components that may not store, process, or transmit CHD/SAD but have unrestricted connectivity to system components that store, process, or transmit CHD/SAD.
CERT	Acronym for “Computer Emergency Response Team.”
Change Control	Processes and procedures to review, test, and approve changes to systems and software for impact before implementation.
CIS	Acronym for “Center for Internet Security.”
Cleartext Data	Unencrypted data.
Column-Level Database Encryption	Technique or technology (either software or hardware) for encrypting contents of a specific column in a database versus the full contents of the entire database. Alternatively, see *Disk Encryption* and *File-Level Encryption*.
Commercial Off-the-Shelf (COTS)	Description of products that are stock items not specifically customized or designed for a specific customer or user and are readily available for use.
Compensating Controls	See PCI DSS Appendices B and C.
Compromise	Also referred to as “data compromise” or “data breach.” Intrusion into a computer system where unauthorized disclosure/theft, modification, or destruction of cardholder data is suspected.
Console	Directly connected screen and/or keyboard which permits access and control of a server, mainframe computer, or other system type. See *Non-Console Access*.

Exhibit 22A-15

Term	Definition
Consumer	Individual cardholder purchasing goods, services, or both.
Critical systems	A system or technology that is deemed by the entity to be of particular importance. For example, a critical system may be essential for the performance of a business operation or for a security function to be maintained. Examples of critical systems often include security systems, public-facing devices and systems, databases, and systems that store, process, or transmit cardholder data.
Cryptographic Algorithm	Also referred to as "encryption algorithm." A clearly specified reversible mathematical process used for transforming cleartext data to encrypted data, and vice versa. See *Strong Cryptography.*
Cryptographic Key	A parameter used in conjunction with a cryptographic algorithm that is used for operations such as: • Transforming cleartext data into ciphertext data, • Transforming ciphertext data into cleartext data, • A digital signature computed from data, • Verifying a digital signature computed from data, • An authentication code computed from data, or • An exchange agreement of a shared secret. See *Strong Cryptography.*
Cryptographic Key Generation	Key generation is one of the functions within key management. The following documents provide recognized guidance on proper key generation: • *NIST Special Publication 800-133: Recommendation for Cryptographic Key Generation* • *ISO 11568-2 Financial services — Key management (retail) — Part 2: Symmetric ciphers, their key management and life cycle* – 4.3 Key generation • *ISO 11568-4 Financial services — Key management (retail) — Part 4: Asymmetric cryptosystems — Key management and life cycle* – 6.2 Key life cycle stages — Generation • *European Payments Council EPC 342-08 Guidelines on Algorithms Usage and Key Management* – 4.1.1 Key generation [for symmetric algorithms] – 4.2.1 Key generation [for asymmetric algorithms].
Cryptographic Key Management	The set of processes and mechanisms which support cryptographic key establishment and maintenance, including replacing older keys with new keys as necessary.

Exhibit 22A-15

Term	Definition
Cryptoperiod	The time span during which a cryptographic key can be used for its defined purpose. Often defined in terms of the period for which the key is active and/or the amount of ciphertext that has been produced by the key, and according to industry best practices and guidelines (for example, *NIST Special Publication 800-57*).
Customized Approach	See PCI DSS section: *8 Approaches for Implementing and Validating PCI DSS.*
CVSS	Acronym for "Common Vulnerability Scoring System." Refer to *ASV Program Guide* for more information.
Data-Flow Diagram	A diagram showing how and where data flows through an entity's applications, systems, networks, and to/from external parties.
Default Account	Login account predefined in a system, application, or device to permit initial access when system is first put into service. Additional default accounts may also be generated by the system as part of the installation process.
Default Password	Password on system administration, user, or service accounts predefined in a system, application, or device; usually associated with default account. Default accounts and passwords are published and well known, and therefore easily guessed.
Defined Approach	See PCI DSS section: *8 Approaches for Implementing and Validating PCI DSS.*
Disk Encryption	Technique or technology (either software or hardware) for encrypting all stored data on a device (for example, a hard disk or flash drive). Alternatively, File-Level Encryption or Column-Level Database Encryption is used to encrypt contents of specific files or columns.
DMZ	Abbreviation for "demilitarized zone." Physical or logical sub-network that provides an additional layer of security to an organization's internal private network.
DNS	Acronym for "Domain Name System."
Dual Control	Process of using two or more separate entities (usually persons) operating in concert to protect sensitive functions or information. Both entities are equally responsible for the physical protection of materials involved in vulnerable transactions. No single person is permitted to access or use the materials (for example, the cryptographic key). For manual key generation, conveyance, loading, storage, and retrieval, dual control requires dividing knowledge of the key among the entities. See *Split Knowledge*.
ECC	Acronym for "Elliptic Curve Cryptography." See *Strong Cryptography*.
E-commerce (web) Redirection Server	A server that redirects a customer browser from a merchant's website to a different location for payment processing during an ecommerce transaction.

Exhibit 22A-15

Term	Definition
Encryption	The (reversible) transformation of data by a cryptographic algorithm to produce cipher text, i.e., to hide the information content of the data. See *Strong Cryptography*.
Encryption Algorithm	See *Cryptographic Algorithm*.
Entity	In the context of a PCI DSS assessment, a term used to represent the corporation, organization, or business which is undergoing an assessment.
File Integrity Monitoring (FIM)	A change-detection solution that checks for changes, additions, and deletions to critical files, and notifies when such changes are detected.
File-Level Encryption	Technique or technology (either software or hardware) for encrypting the full contents of specific files. Alternatively, see *Disk Encryption* and *Column-Level Database Encryption*.
Firewall	Hardware and/or software technology that protects network resources from unauthorized access. A firewall permits or denies computer traffic between networks with different security levels based upon a set of rules and other criteria.
Forensics	Also referred to as "computer forensics." As it relates to information security, the application of investigative tools and analysis techniques to gather evidence from computer resources to determine the cause of data compromises. Investigations into compromises of payment data are typically conducted by a PCI Forensic Investigator (PFI).
FTP	Acronym for "File Transfer Protocol." Network protocol used to transfer data from one computer to another through a public network such as the Internet. FTP is widely viewed as an insecure protocol because passwords and file contents are sent unprotected and in cleartext. FTP can be implemented securely via SSH or other technology.
Hashing	A method to protect data that converts data into a fixed-length message digest. Hashing is a one-way (mathematical) function in which a non-secret algorithm takes any arbitrary length message as input and produces a fixed length output (usually called a "hash code" or "message digest"). Hash functions are required to have the following properties: • It is computationally infeasible to determine the original input given only the hash code, • It is computationally infeasible to find two inputs that give the same hash code.
HSM	Acronym for "hardware security module" or "host security module." A physically and logically protected hardware device that provides a secure set of cryptographic services, used for cryptographic key-management functions and/or the decryption of account data.
IDS	Acronym for "intrusion-detection system."

Exhibit 22A-15

Term	Definition
Index Token	A random value from a table of random values that corresponds to a given PAN.
Interactive Login	The process of an individual providing authentication credentials to directly log into an application or system account. Using interactive login means there is no accountability or traceability of actions taken by that individual.
IPS	Acronym for “intrusion prevention system.”
ISO	Acronym for “International Organization for Standardization.”
Issuer	Also referred to as “issuing bank” or “issuing financial institution.” Entity that issues payment cards or performs, facilitates, or supports issuing services, including but not limited to issuing banks and issuing processors.
Issuing services	Examples of issuing services include but are not limited to authorization and card personalization.
Keyed Cryptographic Hash	A hashing function that incorporates a randomly generated secret key to provide brute force attack resistance and secret authentication integrity. Appropriate keyed cryptographic hashing algorithms include but are not limited to: HMAC, CMAC, and GMAC, with an effective cryptographic strength of at least 128-bits (*NIST SP 800-131Ar2)*. Refer to the following for more information about HMAC, CMAC, and GMAC, respectively: *NIST SP 800-107r1, NIST SP 800-38B, and NIST SP 800-38D).* See *NIST SP 800-107 (Revision 1): Recommendation for Applications Using Approved Hash Algorithms* §5.3.
Key Custodian	A role where a person(s) is entrusted with, and responsible for, performing key management duties involving secret and/or private keys, key shares, or key components on behalf of an entity.
Key Management System	A combination of hardware and software that provides an integrated approach for generating, distributing, and/or managing cryptographic keys for devices and applications.
LAN	Acronym for “local area network.”
LDAP	Acronym for “Lightweight Directory Access Protocol.”
Least Privileges	The minimum level of privileges necessary to perform the roles and responsibilities of the job function.

Exhibit 22A-15

Term	Definition
Legal Exception	A legal restriction due to a local or regional law, regulation, or regulatory requirement, where meeting a PCI DSS requirement would violate that law, regulation, or regulatory requirement. Contractual obligations or legal advice are **not** legal restrictions. See the following PCI DSS v4.x documents for information on reporting legal exceptions: • *The Report on Compliance (ROC) Template* and related *Attestations of Compliance*. • *The Self-Assessment Questionnaires (SAQs)* and related *Attestations of Compliance*. *Note: Where an entity operates in multiple locations, a legal exception may only be claimed for the locations governed by the law, regulation, or regulatory requirement, and may not be claimed for locations in which such law, regulation, or regulatory requirement is inapplicable.*
Log	See *Audit Log*.
Logical Access Control	Mechanisms that limit the availability of information or information-processing resources only to authorized persons or applications. See *Physical Access Control*.
MAC	In cryptography, an acronym for “message authentication code.” See *Strong Cryptography*.
Magnetic-Stripe Data	See *Track Data*.
Masking	Method of concealing a segment of PAN when displayed or printed. Masking is used when there is no business need to view the entire PAN. Masking relates to protection of PAN when displayed on screens, paper receipts, printouts, etc. See *Truncation* for protection of PAN when electronically stored, processed, or transmitted.
Media	Physical material, including but not limited to, electronic storage devices, removable electronic media, and paper reports.
Merchant	For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any PCI SSC Participating Payment Brand as payment for goods and/or services. A merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers. For example, an ISP is a merchant that accepts payment cards for monthly billing, but also is a service provider if it hosts merchants as customers.
MO/TO	Acronym for “Mail-Order/Telephone-Order.”
Multi-Factor Authentication	Method of authenticating a user whereby at least two factors are verified. These factors include something the user has (such as a smart card or dongle), something the user knows (such as a password, passphrase, or PIN), or something the user is or does (such as fingerprints and other biometric elements).

Exhibit 22A-15

Term	Definition
Multi-Tenant Service Provider	A type of Third-Party Service Provider that offers various shared services to merchants and other service providers, where customers share system resources (such as physical or virtual servers), infrastructure, applications (including Software as a Service (SaaS)), and/or databases. Services may include, but are not limited to, hosting multiple entities on a single shared server, providing e-commerce and/or “shopping cart” services, web-based hosting services, payment applications, various cloud applications and services, and connections to payment gateways and processors. See *Service Provider* and *Third-Party Service Provider*.
NAC	Acronym for “Network Access Control.”
NAT	Acronym for “Network Address Translation.”
Network Connection	A logical, physical, or virtual communication path between devices that allows the transmission and reception of network layer packets.
Network Diagram	A diagram showing system components and connections within a networked environment.
Network Security Controls (NSC)	Firewalls and other network security technologies that act as network policy enforcement points. NSCs typically control network traffic between two or more logical or physical network segments (or subnets) based on pre-defined policies or rules.
NIST	Acronym for “National Institute of Standards and Technology.” Non-regulatory federal agency within U.S. Commerce Department's Technology Administration.
Non-Console Access	Logical access to a system component that occurs over a network interface rather than via a direct, physical connection to the system component. Non-console access includes access from within local/internal networks as well as access from external or remote networks.
NTP	Acronym for “Network Time Protocol.”
Organizational Independence	An organizational structure that ensures there is no conflict of interest between the person or department performing the activity and the person or department assessing the activity. For example, individuals performing assessments are organizationally separate from the management of the environment being assessed.
OWASP	Acronym for “Open Web Application Security Project.”
PAN	Acronym for “primary account number.” Unique payment card number (credit, debit, or prepaid cards, etc.) that identifies the issuer and the cardholder account.

Exhibit 22A-15

Term	Definition
Password / Passphrase	A string of characters that serve as an authentication factor for a user or account.
Patch	Update to existing software to add function or to correct a defect.
Participating Payment Brand	Also referred to as "payment brand." A payment card brand that, as of the time in question, is then formally admitted as (or an affiliate of) a member of PCI SSC pursuant to its governing documents. At the time of writing, Participating Payment Brands include PCI SSC Founding Members and Strategic Members.
Payment Brand	An organization with branded payment cards or other payment card form factors. Payment brands regulate where and how the payment cards or other form factors carrying its brand or logo are used. A payment brand may be a PCI SSC Participating Payment Brand or other global or regional payment brand, scheme, or network.
Payment Card Form Factor	Includes physical payment cards as well as devices with functionality that emulates a payment card to initiate a payment transaction. Examples of such devices include, but are not limited to, smartphones, smartwatches, fitness bands, key tags, and wearables such as jewelry.
Payment Cards	For purposes of PCI DSS, any payment card form factor that bears the logo of any PCI SSC Participating Payment Brand.
Payment Channel	Methods used by merchants to accept payments from customers. Common payment channels include card present (in person) and card not present (e-commerce and MO/TO).
Payment Page	A web-based user interface containing one or more form elements intended to capture account data from a consumer or submit captured account data, for purposes of processing and authorizing payment transactions. The payment page can be rendered as any one of: • A single document or instance, • A document or component displayed in an inline frame within a non-payment page, • Multiple documents or components each containing one or more form elements contained in multiple inline frames within a non-payment page.
Payment Page Scripts	Any programming language commands or instructions on a payment page that are processed and/or interpreted by a consumer's browser, including commands or instructions that interact with a page's document object model. Examples of programming languages are JavaScript and VB script; neither markup-languages (for example, HTML) or style-rules (for example, CSS) are programming languages.

Exhibit 22A-15

Term	Definition
Payment Processor	Sometimes referred to as “payment gateway” or “payment service provider (PSP).” Entity engaged by a merchant or other entity to handle payment card transactions on their behalf. See *Acquirers.*
PCI DSS	Acronym for “Payment Card Industry Data Security Standard.”
Personnel	Full-time and part-time employees, temporary employees, contractors, and consultants with security responsibilities for protecting account data or that can impact the security of cardholder data and/or sensitive authentication data. See *Visitor.*
Phishing Resistant Authentication	Authentication designed to prevent the disclosure and use of authentication secrets to any party that is not the legitimate system to which the user is attempting to authenticate (for example, through in-the-middle (ITM) or impersonation attacks). Phishing-resistant systems often implement asymmetric cryptography as a core security control. Systems that rely solely on knowledge-based or time-limited factors such as passwords or one-time-passwords (OTPs) are not considered phishing resistant, nor are SMS or magic links. Examples of phishing-resistant authentication includes FIDO2.
Physical Access Control	Mechanisms that limit the access to a physical space or environment to only authorized persons. See *Logical Access Control*.
PIN	Acronym for “personal identification number.”
PIN Block	A block of data used to encapsulate a PIN during processing. The PIN block format defines the content of the PIN block and how it is processed to retrieve the PIN. The PIN block is composed of the PIN, the PIN length, and may contain the PAN (or a truncation thereof) depending on the approved ISO PIN Block Format used.
POI	Acronym for “Point of Interaction,” the initial point where data is read from a card.
Point of Sale System (POS)	Hardware and software used by merchants to accept payments from customers. May include POI devices, PIN pads, electronic cash registers, etc.
Privileged User	Any user account with greater than basic access privileges. Typically, these accounts have elevated or increased privileges with more rights than a standard user account. However, the extent of privileges across different privileged accounts can vary greatly depending on the organization, job function or role, and the technology in use.
QIR	Acronym for “Qualified Integrator or Reseller.” Refer to the *QIR Program Guide* on the PCI SSC website for more information.

Exhibit 22A-15

Term	Definition
QSA	Acronym for “Qualified Security Assessor.” QSA companies are qualified by PCI SSC to validate an entity’s adherence to PCI DSS requirements. Refer to the *QSA Qualification Requirements* for details about requirements for QSA Companies and Employees.
Remote Access	Access to an entity’s network from a location outside of that network. An example of technology for remote access is a VPN.
Removable Electronic Media	Media that stores digitized data that can be easily removed and/or transported from one computer system to another. Examples of removable electronic media include CD-ROM, DVD-ROM, USB flash drives, and external/portable hard drives. In this context, removable electronic media does not include hot-swappable drives, tape drives used for bulk back-ups, or other media not typically used to transport data from one location for use in another.
Risk Assessment	Enterprise-wide process that identifies valuable system resources and threats; quantifies loss exposures (that is, loss potential) based on estimated frequencies and costs of occurrence; and (optionally) recommends how to allocate resources to countermeasures to minimize total exposure. See *Targeted Risk Analysis*.
Risk Ranking	Process of classifying risks to identify, prioritize, and address items in the order of importance.
ROC	Acronym for “Report on Compliance.” Reporting tool used to document detailed results from an entity’s PCI DSS assessment.
RSA	Algorithm for public-key encryption. See *Strong Cryptography*.
SAQ	Acronym for “Self-Assessment Questionnaire.” Reporting tool used to document self-assessment results from an entity’s PCI DSS assessment.
Scoping	Process of identifying all system components, people, and processes to be included in a PCI DSS assessment. See PCI DSS section: *4 Scope of PCI DSS Requirements*.
Secure Coding	The process of creating and implementing applications that are resistant to tampering and/or compromise.
Security Event	An occurrence considered by an organization to have potential security implications to a system or its environment. In the context of PCI DSS, security events identify suspicious or anomalous activity.
Security Officer	Primary person responsible for an entity’s security.
Segmentation	Also referred to as “network segmentation” or “isolation.” Segmentation isolates system components that store, process, or transmit cardholder data from systems that do not. See “Segmentation” in PCI DSS section: *4 Scope of PCI DSS Requirements*.

Exhibit 22A-15

Term	Definition
Sensitive Area	A sensitive area is typically a subset of the CDE and is any area that houses systems considered critical to the CDE. This includes data centers, server rooms, back-office rooms at retail locations, and any area that concentrates or aggregates cardholder data storage, processing, or transmission. Sensitive areas also include areas housing systems that manage or maintain the security of the CDE (for example, those providing network security controls or that manage physical or logical security). This excludes the areas where only point-of-sale terminals are present, such as the cashier areas in a retail store or call centers where agents are taking payments.
Sensitive Authentication Data (SAD)	Security-related information used to authenticate cardholders and/or authorize payment card transactions. This information includes, but is not limited to, card verification codes, full track data (from magnetic stripe or equivalent on a chip), PINs, and PIN blocks.
Separation of Duties	Practice of dividing steps in a function among multiple individuals, to prevent a single individual from subverting the process.
Service Code	Three-digit or four-digit value in the magnetic-stripe that follows the expiration date of the payment card on the track data. It is used for various things, such as defining service attributes, differentiating between international and national interchange, or identifying usage restrictions.
Service Provider	Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data (CHD) and/or sensitive authentication data (SAD) on behalf of another entity. This includes payment gateways, payment service providers (PSPs), and independent sales organizations (ISOs). This also includes companies that provide services that control or could impact the security of CHD and/or SAD. Examples include managed service providers that provide managed firewalls, IDS, and other services as well as hosting providers and other entities. If an entity provides a service that involves *only* the provision of public network access—such as a telecommunications company providing just the communication link—the entity would not be considered a service provider for that service (although they may be considered a service provider for other services). See *Multi-Tenant Service Provider* and *Third-Party Service Provider.*
SNMP	Acronym for “Simple Network Management Protocol.”.
Split Knowledge	A method by which two or more entities separately have key components or key shares that individually convey no knowledge of the resultant cryptographic key.
SQL	Acronym for “Structured Query Language.”
SSH	Abbreviation for “Secure Shell.”
SSL	Acronym for “Secure Sockets Layer.”

Exhibit 22A-15

Term	Definition
Strong Cryptography	Cryptography is a method to protect data through a reversible encryption process, and is a foundational primitive used in many security protocols and services. Strong cryptography is based on industry-tested and accepted algorithms along with key lengths that provide a minimum of 112-bits of effective key strength and proper key-management practices. Effective key strength can be shorter than the actual 'bit' length of the key, which can lead to algorithms with larger keys providing lesser protection than algorithms with smaller actual, but larger effective, key sizes. *It is recommended that all new implementations use a minimum of 128-bits of effective key strength.* Examples of industry references on cryptographic algorithms and key lengths include: • *NIST Special Publication 800-57 Part 1,* • *BSI TR-02102-1,* • *ECRYPT-CSA D5.4 Algorithms, Key Size and Protocols Report (2018), and* • *ISO/IEC 18033 Encryption algorithms, and* • *ISO/IEC 14888-3:2-81 IT Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms*.
System Components	Any network devices, servers, computing devices, virtual components, or software included in or connected to the CDE, or that could impact the security of cardholder data and/or sensitive authentication data.
System-level object	Anything on a system component that is required for its operation, including but not limited to application executables and configuration files, system configuration files, static and shared libraries and DLLs, system executables, device drivers and device configuration files, and third-party components.
Targeted Risk Analysis	For PCI DSS purposes, a risk analysis that focuses on a specific PCI DSS requirement(s) of interest, either because the requirement allows flexibility (for example, as to frequency) or, for the Customized Approach, to explain how the entity assessed the risk and determined the customized control meets the objective of a PCI DSS requirement.
TDES	Acronym for "Triple Data Encryption Standard." Also referred to as "3DES" or "Triple DES."
Telnet	Abbreviation for "telephone network protocol."
Third-Party Service Provider (TPSP)	Any third party acting as a service provider on behalf of an entity. See *Multi-Tenant Service Provider* and *Service Provider*.
Third-Party Software	Software that is acquired by, but not developed expressly for, an entity. It may be open source, freeware, shareware, or purchased.
TLS	Acronym for "Transport Layer Security."

Exhibit 22A-15

Term	Definition
Token	In the context of authentication and access control, a token is a value provided by hardware or software that works with an authentication server or VPN to perform dynamic or multi-factor authentication.
Track Data	Also referred to as “full track data” or “magnetic-stripe data.” Data encoded in the magnetic stripe or chip used for authentication and/or authorization during payment transactions. Can be the magnetic-stripe image on a chip or the track data on the magnetic stripe.
Truncation	Method of rendering a full PAN unreadable by removing a segment of PAN data. Truncation relates to protection of PAN when electronically stored, processed, or transmitted. See *Masking* for protection of PAN when displayed on screens, paper receipts, etc.
Trusted Network	Network of an entity that is within the entity’s ability to control or manage and that meets applicable PCI DSS requirements.
Untrusted Network	Any network that does not meet the definition of a “trusted network.”
Virtual Payment Terminal	In the context of Self-Assessment Questionnaire (SAQ) C-VT, a virtual payment terminal is web-browser-based access to an acquirer, processor, or third-party service provider website to authorize payment card transactions, where the merchant manually enters payment card data through a web browser. Unlike physical terminals, virtual payment terminals do not read data directly from a payment card. Because payment card transactions are entered manually, virtual payment terminals are typically used instead of physical terminals in merchant environments with low transaction volumes.
Virtualization	The logical abstraction of computing resources from physical and/or logical constraints. One common abstraction is referred to as virtual machines or VMs, which takes the content of a physical machine and allows it to operate on different physical hardware and/or along with other virtual machines on the same physical hardware. Other common abstractions include, but are not limited to, containers, serverless computing, or microservices.
Visitor	A vendor, guest of any personnel, service worker, or personnel that normally do not have access to the subject area. Cardholders present in a retail location to purchase goods or services are not considered “visitors.” See *Cardholder* and *Personnel.*
VPN	Acronym for “virtual private network.”
Vulnerability	Flaw or weakness which, if exploited, may result in an intentional or unintentional compromise of a system.
Web Application	An application that is generally accessed through a web browser or through web services. Web applications may be available through the Internet or a private, internal network.

Exhibit 22A-16

Requirements and Testing Procedures		Guidance
3.6 Cryptographic keys used to protect stored account data are secured.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Cryptographic keys must be strongly protected because those who obtain access will be able to decrypt data. **Good Practice** Having a centralized key management system based on industry standards is recommended for managing cryptographic keys. **Further Information** The entity's key management procedures will benefit through alignment with industry requirements, Sources for information on cryptographic key management life cycles include: • *ISO 11568-1 Banking — Key management (retail) — Part 1*: Principles (specifically Chapter 10 and the referenced Parts 2 & 4) • *NIST SP 800-57 Part 1 Revision 5— Recommendation for Key Management, Part 1: General*.
3.6.1 Procedures are defined and implemented to protect cryptographic keys used to protect stored account data against disclosure and misuse that include: • Access to keys is restricted to the fewest number of custodians necessary. • Key-encrypting keys are at least as strong as the data-encrypting keys they protect. • Key-encrypting keys are stored separately from data-encrypting keys. • Keys are stored securely in the fewest possible locations and forms.	**3.6.1** Examine documented key-management policies and procedures to verify that processes to protect cryptographic keys used to protect stored account data against disclosure and misuse are defined to include all elements specified in this requirement.	
Customized Approach Objective		
Processes that protect cryptographic keys used to protect stored account data against disclosure and misuse are defined and implemented.		
Applicability Notes		
This requirement applies to keys used to protect stored account data and to key-encrypting keys used to protect data-encrypting keys. The requirement to protect keys used to protect stored account data from disclosure and misuse applies to both data-encrypting keys and key-encrypting keys. Because one key-encrypting key may grant access to many data-encrypting keys, the key-encrypting keys require strong protection measures.		

Exhibit 22A-16

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Maintaining current documentation of the cryptographic architecture enables an entity to understand the algorithms, protocols, and cryptographic keys used to protect stored account data, as well as the devices that generate, use, and protect the keys. This allows an entity to keep pace with evolving threats to its architecture and plan for updates as the assurance level provided by different algorithms and key strengths changes. Maintaining such documentation also allows an entity to detect lost or missing keys or key-management devices and identify unauthorized additions to its cryptographic architecture. The use of the same cryptographic keys in both production and test environments introduces a risk of exposing the key if the test environment is not at the same security level as the production environment. **Good Practice** Having an automated reporting mechanism can assist with maintenance of the cryptographic attributes.
3.6.1.1 ***Additional requirement for service providers only:*** A documented description of the cryptographic architecture is maintained that includes: • Details of all algorithms, protocols, and keys used for the protection of stored account data, including key strength and expiry date. • Preventing the use of the same cryptographic keys in production and test environments. *This bullet is a best practice until its effective date; refer to Applicability Notes below for details.* • Description of the key usage for each key. • Inventory of any hardware security modules (HSMs), key management systems (KMS), and other secure cryptographic devices (SCDs) used for key management, including type and location of devices, to support meeting Requirement 12.3.4.	**3.6.1.1** ***Additional testing procedure for service provider assessments only:*** Interview responsible personnel and examine documentation to verify that a document exists to describe the cryptographic architecture that includes all elements specified in this requirement.	
Customized Approach Objective		
Accurate details of the cryptographic architecture are maintained and available. *(continued on next page)*		

Exhibit 22A-16

Requirements and Testing Procedures		Guidance
Applicability Notes		
This requirement applies only when the entity being assessed is a service provider. In cloud HSM implementations, responsibility for the cryptographic architecture according to this Requirement will be shared between the cloud provider and the cloud customer. *The bullet above (for including, in the cryptographic architecture, that the use of the same cryptographic keys in production and test is prevented) is a best practice until 31 March 2025, after which it will be required as part of Requirement 3.6.1.1 and must be fully considered during a PCI DSS assessment.*		

Exhibit 22A-16

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Storing cryptographic keys securely prevents unauthorized or unnecessary access that could result in the exposure of stored account data. Storing keys separately means they are stored such that if the location of one key is compromised, the second key is not also compromised. **Good Practice** Where data-encrypting keys are stored in an HSM, the HSM interaction channel should be protected to prevent interception of encryption or decryption operations.
3.6.1.2 Secret and private keys used to protect stored account data are stored in one (or more) of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. • Within a secure cryptographic device (SCD), such as a hardware security module (HSM) or PTS-approved point-of-interaction device. • As at least two full-length key components or key shares, in accordance with an industry-accepted method.	**3.6.1.2.a** Examine documented procedures to verify it is defined that cryptographic keys used to encrypt/decrypt stored account data must exist only in one (or more) of the forms specified in this requirement.	
	3.6.1.2.b Examine system configurations and key storage locations to verify that cryptographic keys used to encrypt/decrypt stored account data exist in one (or more) of the forms specified in this requirement.	
	3.6.1.2.c Wherever key-encrypting keys are used, examine system configurations and key storage locations to verify: • Key-encrypting keys are at least as strong as the data-encrypting keys they protect. • Key-encrypting keys are stored separately from data-encrypting keys.	
Customized Approach Objective		
Secret and private keys are stored in a secure form that prevents unauthorized retrieval or access. *(continued on next page)*		

Exhibit 22A-16

Requirements and Testing Procedures		Guidance
Applicability Notes It is not required that public keys be stored in one of these forms. Cryptographic keys stored as part of a key management system (KMS) that employs SCDs are acceptable. A cryptographic key that is split into two parts does not meet this requirement. Secret or private keys stored as key components or key shares must be generated via one of the following: • Using an approved random number generator and within an SCD, **OR** • According to ISO 19592 or equivalent industry standard for generation of secret key shares.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Restricting the number of people who have access to cleartext cryptographic key components reduces the risk of stored account data being retrieved or rendered visible by unauthorized parties. **Good Practice** Only personnel with defined key custodian responsibilities (creating, altering, rotating, distributing, or otherwise maintaining encryption keys) should be granted access to key components. Ideally this will be a very small number of people.
3.6.1.3 Access to cleartext cryptographic key components is restricted to the fewest number of custodians necessary.	**3.6.1.3** Examine user access lists to verify that access to cleartext cryptographic key components is restricted to the fewest number of custodians necessary.	
Customized Approach Objective Access to cleartext cryptographic key components is restricted to necessary personnel.		

Exhibit 22A-16

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Storing any cryptographic keys in the fewest locations helps an organization track and monitor all key locations and minimizes the potential for keys to be exposed to unauthorized parties.
3.6.1.4 Cryptographic keys are stored in the fewest possible locations.	**3.6.1.4** Examine key storage locations and observe processes to verify that keys are stored in the fewest possible locations.	
Customized Approach Objective		
Cryptographic keys are retained only where necessary.		

Exhibit 22A-16

Requirements and Testing Procedures		Guidance
3.7 Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are defined and implemented.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Use of strong cryptographic keys significantly increases the level of security of encrypted account data. **Further Information** See the sources referenced at Cryptographic Key Generation in *Appendix G*.
3.7.1 Key-management policies and procedures are implemented to include generation of strong cryptographic keys used to protect stored account data.	**3.7.1.a** Examine the documented key-management policies and procedures for keys used for protection of stored account data to verify that they define generation of strong cryptographic keys.	
	3.7.1.b Observe the method for generating keys to verify that strong keys are generated.	
Customized Approach Objective		
Strong cryptographic keys are generated.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Secure distribution or conveyance of secret or private cryptographic keys means that keys are distributed only to authorized custodians, as identified in Requirement 3.6.1.2, and are never distributed insecurely.
3.7.2 Key-management policies and procedures are implemented to include secure distribution of cryptographic keys used to protect stored account data.	**3.7.2.a** Examine the documented key-management policies and procedures for keys used for protection of stored account data to verify that they define secure distribution of cryptographic keys.	
	3.7.2.b Observe the method for distributing keys to verify that keys are distributed securely.	
Customized Approach Objective		
Cryptographic keys are secured during distribution.		

Exhibit 22A-16

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Storing keys without proper protection could provide access to attackers, resulting in the decryption and exposure of account data. **Good Practice** Data encryption keys can be protected by encrypting them with a key-encrypting key. Keys can be stored in a Hardware Security Module (HSM). Secret or private keys that can decrypt data should never be present in source code.
3.7.3 Key-management policies and procedures are implemented to include secure storage of cryptographic keys used to protect stored account data.	**3.7.3.a** Examine the documented key-management policies and procedures for keys used for protection of stored account data to verify that they define secure storage of cryptographic keys.	
	3.7.3.b Observe the method for storing keys to verify that keys are stored securely.	
Customized Approach Objective		
Cryptographic keys are secured when stored.		

Exhibit 22A-16

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Changing encryption keys when they reach the end of their cryptoperiod is imperative to minimize the risk of someone obtaining the encryption keys and using them to decrypt data. **Definitions** A cryptoperiod is the time span during which a cryptographic key can be used for its defined purpose. Cryptoperiods are often defined in terms of the period for which the key is active and/or the amount of cipher-text that has been produced by the key. Considerations for defining the cryptoperiod include, but are not limited to, the strength of the underlying algorithm, size or length of the key, risk of key compromise, and the sensitivity of the data being encrypted. **Further Information** *NIST SP 800-57 Part 1, Revision 5, Section 5.3 Cryptoperiods* – provides guidance for establishing the time span during which a specific key is authorized for use by legitimate entities, or the keys for a given system will remain in effect. See Table 1 of *SP 800-57* Part 1 for suggested cryptoperiods for different key types.
3.7.4 Key management policies and procedures are implemented for cryptographic key changes for keys that have reached the end of their cryptoperiod, as defined by the associated application vendor or key owner, and based on industry best practices and guidelines, including the following: • A defined cryptoperiod for each key type in use. • A process for key changes at the end of the defined cryptoperiod.	**3.7.4.a** Examine the documented key-management policies and procedures for keys used for protection of stored account data to verify that they define changes to cryptographic keys that have reached the end of their cryptoperiod and include all elements specified in this requirement.	
	3.7.4.b Interview personnel, examine documentation, and observe key storage locations to verify that keys are changed at the end of the defined cryptoperiod(s).	
Customized Approach Objective		
Cryptographic keys are not used beyond their defined cryptoperiod.		

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Keys that are no longer required, keys with weakened integrity, and keys that are known or suspected to be compromised, should be archived, revoked, and/or destroyed to ensure that the keys can no longer be used. If such keys need to be kept (for example, to support archived encrypted data), they should be strongly protected. **Good Practice** Archived cryptographic keys should be used only for decryption/verification purposes. The encryption solution should provide for and facilitate a process to replace keys that are due for replacement or that are known to be, or suspected of being, compromised. In addition, any keys that are known to be, or suspected of being, compromised should be managed in accordance with the entity's incident response plan per Requirement 12.10.1. **Further Information** Industry best practices for archiving retired keys are outlined in *NIST SP 800-57 Part 1, Revision 5, Section 8.3.1*, and includes maintaining the archive with a trusted third party and storing archived key information separately from operational data.
3.7.5 Key management policies procedures are implemented to include the retirement, replacement, or destruction of keys used to protect stored account data, as deemed necessary when: • The key has reached the end of its defined cryptoperiod. • The integrity of the key has been weakened, including when personnel with knowledge of a cleartext key component leaves the company, or the role for which the key component was known. • The key is suspected of or known to be compromised. Retired or replaced keys are not used for encryption operations.	**3.7.5.a** Examine the documented key-management policies and procedures for keys used for protection of stored account data and verify that they define retirement, replacement, or destruction of keys in accordance with all elements specified in this requirement. **3.7.5.b** Interview personnel to verify that processes are implemented in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Keys are removed from active use when it is suspected or known that the integrity of the key is weakened.		
Applicability Notes		
If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key).		

Exhibit 22A-16

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Split knowledge and dual control of keys are used to eliminate the possibility of a single person having access to the whole key and therefore being able to gain unauthorized access to the data. **Definitions** Split knowledge is a method in which two or more people separately have key components, where each person knows only their own key component, and the individual key components convey no knowledge of other components or of the original cryptographic key. Dual control requires two or more people to authenticate the use of a cryptographic key or perform a key-management function. No single person can access or use the authentication factor (for example, the password, PIN, or key) of another. **Good Practice** Where key components or key shares are used, procedures should ensure that no single custodian ever has access to sufficient key components or shares to reconstruct the cryptographic key. For example, in an m-of-n scheme (for example, Shamir), where only two of any three components are required to reconstruct the cryptographic key, a custodian must not have current or prior knowledge of more than one component. If a custodian was previously assigned component A, which was then reassigned, the custodian should not then be assigned component B or C, as this would give the custodian knowledge of two components and the ability to recreate the key. *(continued on next page)*
3.7.6 Where manual cleartext cryptographic key-management operations are performed by personnel, key-management policies and procedures are implemented, including managing these operations using split knowledge and dual control.	**3.7.6.a** Examine the documented key-management policies and procedures for keys used for protection of stored account data and verify that they define using split knowledge and dual control. **3.7.6.b** Interview personnel and/or observe processes to verify that manual cleartext keys are managed with split knowledge and dual control.	
Customized Approach Objective		
Cleartext secret or private keys cannot be known by anyone. Operations involving cleartext keys cannot be carried out by a single person.		
Applicability Notes		
This control is applicable for manual key-management operations. A cryptographic key that is simply split into two parts does not meet this requirement. Secret or private keys stored as key components or key shares must be generated via one of the following: • Using an approved random number generator and within a secure cryptographic device (SCD), such as a hardware security module (HSM) or PTS-approved point-of-interaction device, **OR** • According to ISO 19592 or equivalent industry standard for generation of secret key shares.		

Requirements and Testing Procedures		Guidance
3.7.6 *(continued)*		**Examples** Key-management operations that might be performed manually include, but are not limited to, key generation, transmission, loading, storage, and destruction. **Further Information** Industry standards for managing key components include: • *NIST SP 800-57* Part 2, Revision 1 -- Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations [4.6 Keying Material Distribution] • *ISO 11568-2 Banking — Key management (retail) — Part 2*: Symmetric ciphers, their key management and life cycle [4.7.2.3 Key components and 4.9.3 Key components] • *European Payments Council EPC342-08 Guidelines on Cryptographic Algorithms Usage and Key Management* [especially 4.1.4 Key installation].
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If an attacker is able to substitute an entity's key with a key the attacker knows, the attacker will be able to decrypt all data encrypted with that key. **Good Practice** The encryption solution should not allow for or accept substitution of keys from unauthorized sources or unexpected processes. Controls should include ensuring that individuals with access to key components or shares do not have access to other components or shares that form the necessary threshold to derive the key.
3.7.7 Key management policies and procedures are implemented to include the prevention of unauthorized substitution of cryptographic keys.	**3.7.7.a** Examine the documented key-management policies and procedures for keys used for protection of stored account data and verify that they define prevention of unauthorized substitution of cryptographic keys. **3.7.7.b** Interview personnel and/or observe processes to verify that unauthorized substitution of keys is prevented.	
Customized Approach Objective		
Cryptographic keys cannot be substituted by unauthorized personnel.		

Exhibit 22A-16

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** This process will help ensure individuals that act as key custodians commit to the key-custodian role and understand and accept the responsibilities. An annual reaffirmation can help remind key custodians of their responsibilities. **Further Information** Industry guidance for key custodians and their roles and responsibilities includes: • *NIST SP 800-130 A Framework for Designing Cryptographic Key Management Systems* [5. Roles and Responsibilities (especially) for Key Custodians] • *ISO 11568-1 Banking -- Key management (retail) -- Part 1*: Principles [5 Principles of key management (especially b)]
3.7.8 Key management policies and procedures are implemented to include that cryptographic key custodians formally acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities.	**3.7.8.a** Examine the documented key-management policies and procedures for keys used for protection of stored account data and verify that they define acknowledgments for key custodians in accordance with all elements specified in this requirement.	
	3.7.8.b Examine documentation or other evidence showing that key custodians have provided acknowledgments in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Key custodians are knowledgeable about their responsibilities in relation to cryptographic operations and can access assistance and guidance when required.		

Exhibit 22A-16

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	
3.7.9 ***Additional requirement for service providers only:*** Where a service provider shares cryptographic keys with its customers for transmission or storage of account data, guidance on secure transmission, storage and updating of such keys is documented and distributed to the service provider's customers.	**3.7.9** ***Additional testing procedure for service provider assessments only:*** If the service provider shares cryptographic keys with its customers for transmission or storage of account data, examine the documentation that the service provider provides to its customers to verify it includes guidance on how to securely transmit, store, and update customers' keys in accordance with all elements specified in Requirements 3.7.1 through 3.7.8 above.	**Purpose** Providing guidance to customers on how to securely transmit, store, and update cryptographic keys can help prevent keys from being mismanaged or disclosed to unauthorized entities. **Further Information** Numerous industry standards for key management are cited above in the Guidance for Requirements 3.7.1-3.7.8.
Customized Approach Objective		
Customers are provided with appropriate key management guidance whenever they receive shared cryptographic keys.		
Applicability Notes		
This requirement applies only when the entity being assessed is a service provider.		

Exhibit 9A-1

OHANA GROWTH PARTNERS, LLC 212 West Padonia Road Timonium, Maryland 21093	**IN THE**
Plaintiff,	**CIRCUIT COURT**
	FOR
vs.	**BALTIMORE COUNTY**
RYAN DILLON-CAPPS 1334 Maple Avenue Essex, Maryland 21221	**FILE NO.: ____________________**
Defendant.	

COMPLAINT

Plaintiff, Ohana Growth Partners, LLC. ("Plaintiff" or the "Ohana"), by its undersigned counsel, hereby sues Defendant, Ryan Dillon-Capps ("Defendant" or "Dillon-Capps) and states as follows.

NATURE OF ACTION

1. This is an action brought as a result of Defendant's breaches of their duties as Plaintiff's employee, most significantly in refusing to provide Global Administrator rights, pertaining to Plaintiff's software systems and Internet domain name registrations, to Plaintiff's officers and designees. Instead, Defendant has eliminated all Global Administrator rights other than those Defendant possesses, and through which Defendant currently exercises complete control over those systems and registrations. Because, in addition to constituting breaches of Defendant's duties to Plaintiff, Defendant's actions create a substantial risk to Plaintiff's systems, data and business, Plaintiff seeks an immediate injunction compelling Defendant provide Global Administrator rights to Plaintiff's designee as directed.

Exhibit 9A-1

THE PARTIES

2. Plaintiff Ohana is a Maryland limited liability company with its principal place of business located at 212 West Padonia Road, Timonium, Baltimore County, Maryland 21093.

3. Defendant Dillon-Capps is a citizen of the State of Maryland who resides at 1334 Maple Avenue, Essex, Baltimore County, Maryland.

JURISDICTION AND VENUE

4. The Court has subject matter jurisdiction over this action pursuant to MD. CODE ANN., CTS. & JUD PROC., §1-501.

5. This Court has personal jurisdiction over Defendant pursuant to MD. CODE ANN., CTS. & JUD PROC., §6-102(a) because they reside in Baltimore County, Maryland.

6. Venue is proper in this Circuit pursuant to MD. CODE ANN., CTS. & JUD PROC., §6-201(a) because Defendant resides in Baltimore County.

FACTUAL BACKGROUND

7. Ohana is a franchise division of Planet Fitness. Ohana owns and operates 78 Planet Fitness health clubs with over 500,000 members in Maryland, the District of Columbia, Tennessee, Florida, Washington state, and California.

8. Ohana has 1,472 employees, 712 of whom live in Maryland.

9. Ohana maintains a Microsoft 365 account (the "Ohana MS 365 Account"), through which it provides a full suite of software applications to the company's employees, including Microsoft Exchange for company email, Microsoft OneDrive and SharePoint for document management and storage, Microsoft Teams for videoconferencing, as well as other IT services. Ohana's Microsoft 365 Account also includes a subscription to Microsoft Azure, which

Exhibit 9A-1

provides Ohana the ability to deploy, operate and back up data created with those applications in the cloud.

10. Through an account with Internet domain registrar GoDaddy.com, Ohana maintains and administers registrations for over a dozen second level internet domain names, which are directed to websites and Ohana's Microsoft Exchange company email. (the "Ohana GoDaddy Account").

11. Since February 10, 2020, Ryan Dillon-Capps (*nee* Wagner), the Defendant in the above-captioned matter ("Dillon-Capps"), has been employed by Ohana as its Vice President of Information Technology. On January 9, 2020 Ohana and Dillon-Capps executed an Employment and Non-Disclosure Agreement (the "Dillon-Capps Employment Agreement"). As of at least June 2, 2024 Dillon-Capps asked to be referred to using plural pronouns.

12. Dillon-Capps reports to Glenn Norris, the Chief Financial Officer of Ohana ("Norris"). In that capacity, Norris provides Dillon-Capps with supervision and issues directives in connection with the operation of Ohana's software systems.

13. Ohana granted to Dillon-Capps, in their capacity as Vice President of Information Technology and so that they could perform requested job duties, "Global Admin" rights to the Ohana MS 365 Account, allowing them "almost unlimited access to [Ohana's] settings and most of its data." Because "[a] Global Admin may inadvertently lock their account and require a password reset, . . .[Microsoft] recommend[s] [Ohana] have at least either one more Global Admin." *See* https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide Additionally, it is important that more than one person have full administrative right in case one person holding them is unavailable or, as in this case, refuses to cooperate with company directives regarding the IT system owned by the company. In part for

Exhibit 9A-1

those reasons, Ohana had also provided Global Admin rights to Ryan Brooks of Baltimore Consulting, an independent third-party contractor for Ohana that provides comprehensive IT services.

14. On May 20, 2024, without authorization from Norris or other senior executives, Dillon-Capps severed and discontinued all administrative access to the Ohana MS 365 Account that had been held by other Ohana employees, as well as the Global Admin rights provided to Mr. Brooks. On six (6) separate occasions between May 21, 2024 and May 24, 2024, Dillon-Capps was sent express written directives to reinstate Mr. Brooks' administrative access. Since May 24, 2024, management sent Dillon-Capps separate written directives to provide full administrative rights to Justin Drummond, Ohana's President, to Victor Brick, Ohana's CEO, and to Norris, the CFO, in addition to Mr. Brooks. All these directives were disobeyed. Despite these repeated written express directives from Ohana's management, and in violation of Section 1 of the Dillon-Capps Employment Agreement, Dillon-Capps refused to instate full administrative rights to the Ohana MS 365 Account to Ohana's President, CEO, and CFO.

15. In their capacity as Vice President of Information Technology, Dillon-Capps acquired sole administrative control over the Ohana GoDaddy Account.

16. On June 13, 2024, Ohana's Vice President of Human Resources Richard Hartman sent an email to Mr. Dillon-Capps directing them to provide the Global Administrator rights over the Ohana MS 365 Account to Phil Leadore, of Hartman Executive Advisors, which Ohana engaged to assist Ohana with IT matters, and to do so by 3 pm that day. Mr Dillon-Capps refused to comply with that directive, claiming that Ohana's efforts to control its own systems, MS 365 Account somehow amounts to retaliation against them. Mr. Dillon-Capps failed to comply with the directive by 3 p.m. As a result Dillon-Capps continues to maintain and exercise exclusive

Exhibit 9A-1

administrative rights to the Ohana Microsoft 365 Account and administrative control of the Ohana GoDaddy Account.

17. As of 2:05 p.m. on June 13, 2024, Mr. Hartman discovered that he had been locked out of his Ohana company email account and is now unable to send or receive emails from that account to or from any of Ohana's 1,472 employees. As of 5 p.m. on June 13, 2024 Mr. Hartman discovered that he was unable to log into Ohana's Microsoft Teams account and is effectively locked out of the Microsoft 356 suite of applications in the Ohana MS 365 Account. Mr. Hartman's inability, caused by Dillon-Capps, to communicate with any of Ohana's 1,472 employees or to access any of Ohana's personnel records has effectively rendered it impossible for him to perform in his critical role as Vice President of Human Resources for the company.

18. At 8:45 p.m. on June 13, 2024, at the direction of Ohana President Justin Drummond, Mr. Hartman sent an email to Dillon-Capps, using his personal email account, to which Mr. Hartman attached a letter advising Dillon-Capps of the immediate suspension of their employment with Ohana. Dillon-Capps responded with an email, copying President Justin Drummond and other Ohana executives, stating that Dillon-Capps did not recognize Mr. Hartman's authority as Vice President of Human Resources to suspend Dillon-Capps' employment, and falsely claimed that Dillon-Capps was acting upon Mr. Drummond's authority. Mr. Drummond responded to Dillon-Capps' email as follows:

> Ryan:
>
> Your assertions that Rich Hartman did not suspend you or lacked the authority to suspend you are both incorrect and baseless.
>
> For the avoidance of any doubt by you, I incorporate into this email Rich Hartman's email to you today notifying you of your suspension and hereby confirm that you were suspended upon receipt of that email. Please follow fully the directives in that suspension notification.

Exhibit 9A-1

> I also hereby confirm that you have been directed by me to immediately comply with Rich Hartman's email of 9:01 am this morning by immediately adding Phil Leodore from HEA as a Global Administrator regardless of whether he has confirmed any qualifications or involvement in the PCI DSS v4 review.
>
> Thank You,
>
> *Please excuse any typos. Email sent from iPhone*
>
> **Justin Drummond**

As of the filing of this Complaint Mr. Drummond has received no response from Dillon-Capps, nor has Dillon-Capps complied with the directive to add Phil Leadore from HEA as a Global Administrator on Ohana's Microsoft 365 account.

19. Without administrative rights to the Ohana Microsoft 365 account, Ohana is unable to manage any of its Microsoft 365 software applications and related data. So long as Dillon-Capps continues to hold exclusive Global Admin rights to the Ohana MS 365 Account, and by extension Ohana's employee email accounts and data, those accounts and data are vulnerable to disruption by Dillon-Capps. So long as Dillon-Capps continues to hold exclusive administrative control over the Ohana GoDaddy Account, the direction of Ohana's registered domain names to Ohana's company email and websites are at risk.

20. Even a temporary disruption of the Ohana MS 365 Account and/or the Ohana GoDaddy Account would result in tremendous disruption of Ohana's business operation and irreparable harm to Ohana. Given Dillon-Capps refusal to act as directed by their supervisors and other behavior, Ohana believes that, in the absence of a Court Order directing Dillon-Capps to immediately provide the Global Administrator rights to Phil Leadore there is a significant risk that Dillon-Capps will take action to disrupt Ohana's software systems and business operations and to destroy or corrupt Ohana's data.

Exhibit 9A-1

COUNT I – BREACH OF CONTRACT

21. Ohana incorporates the allegations above as if fully set forth herein.

22. Defendant's repeated refusal to comply with Ohana's directives to provide Global Admin rights to Mr. Leadore and others violates Section 1 of the Dillon-Capps Employment Agreement, which requires that Dillon-Caps "faithfully and diligently perform . . . duties as may be assigned by management from time to time."

23. Defendant's violation and continued violation of the Dillon-Capps Employment Agreement has directly resulted in damages to Ohana in the form of significant expense, including otherwise unnecessary consulting fees and attorneys' fees.

24. Defendant's continued violation of the Dillon-Capps Employment Agreement is depriving Ohana of the right to control Ohana's property, to wit, the Ohana MS 365 Account and the Ohana GoDaddy Account and has created a risk of imminent and irreparable harm to Ohana.

WHEREFORE, Plaintiff, Ohana Growth Partners, LLC, respectfully requests that judgment be entered as to Count I in favor of Ohana and against Defendant in an amount equal to the damages caused by Defendant's wrongful conduct, plus pre- and post-judgment interest thereon; that temporary, preliminary and permanent injunctions be entered requiring Defendant to take immediate action to provide Global Administrator rights over the Ohana MS 365 Account and the Ohana GoDaddy Account to Phil Leadore, of Hartman Executive Advisors; and that the Court award to Ohana the cost of these proceedings, and such other and further relief as this Court deems just and appropriate under the circumstances.

COUNT II – BREACH OF DUTY OF LOYALTY

25. Ohana incorporates the allegations above as if fully set forth herein.

Exhibit 9A-1

26. Defendant's repeated refusal to comply with Ohana's directives to provide Global Admin rights to Mr. Leadore and others violates Dillon-Capps' duty of loyalty to Ohana as their employer.

27. Defendant's violation and continued violation of their duty of loyalty has directly resulted in damages to Ohana in the form of significant expense, including otherwise unnecessary consulting fees and attorneys' fees.

28. Defendant's continued violation of their duty of loyalty is depriving Ohana of the right to control Ohana's property, to wit, the Ohana MS 365 Account and the Ohana GoDaddy Account and has created a risk of imminent and irreparable harm to Ohana.

WHEREFORE, Plaintiff, Ohana Growth Partners, LLC, respectfully requests that judgment be entered as to Count II in favor of Ohana and against Defendant in an amount equal to the damages caused by Defendant's wrongful conduct, plus pre- and post-judgment interest thereon; that temporary, preliminary and permanent injunctions be entered requiring Defendant to take immediate action to provide Global Administrator rights over the Ohana MS 365 Account and the Ohana GoDaddy Account to Phil Leadore, of Hartman Executive Advisors; and that the Court award to Ohana the cost of these proceedings, and such other and further relief as this Court deems just and appropriate under the circumstances.

COUNT III – BREACH OF DUTY OF MD. CODE ANN., CRIM. LAW., §7-302(c)

29. Ohana incorporates the allegations above as if fully set forth herein.

30. Defendant's repeated refusal to comply with Ohana's directives to provide Global Admin rights to Mr. Leadore and others constitutes a violation of MD. CODE ANN., CRIM. LAW., §7-302(c).

Exhibit 9A-1

31. Ohana has suffered a specific and direct injury because of Defendant's violation of and, therefore is entitled, pursuant to MD. CODE ANN., CRIM. LAW., §7-302(g), to bring a civil action against Defendant for that violation to recover Ohana's actual damages and reasonable attorneys' fees and court costs.

32. Defendant's continued violation of MD. CODE ANN., CRIM. LAW., §7-302(c) is depriving Ohana of the right to control Ohana's property, to wit, the Ohana MS 365 Account and the Ohana GoDaddy Account and has created a risk of imminent and irreparable harm to Ohana.

WHEREFORE, Plaintiff, Ohana Growth Partners, LLC, respectfully requests that judgment be entered as to Count III in favor of Ohana and against Defendant in an amount equal to the damages caused by Defendant's wrongful conduct, plus pre- and post-judgment interest thereon and the reasonable attorneys' fees and court costs that Ohana has incurred in connection with this matter; that temporary, preliminary and permanent injunctions be entered requiring Defendant to take immediate action to provide Global Administrator rights over the Ohana MS 365 Account and the Ohana GoDaddy Account to Phil Leadore, of Hartman Executive Advisors; and such other and further relief as this Court deems just and appropriate under the circumstances.

Exhibit 9A-1

Dated: June 14, 2024

/s/ Robert S. Brennen
Robert S. Brennen (AIS # 8712010068)
e-mail: RBrennen@milestockbridge.com
Stephen D. Frenkil (AIS # 7712010110)
e-mail: SFrenkil@milesstockbridge.com
Victoria K. Hoffberger (AIS # 1912170195)
e-mail: VHoffberger@milesstockbridge.com
MILES & STOCKBRIDGE P.C.
100 Light Street
Baltimore, Maryland 21202
Telephone: (410) 727-6464
Facsimile: (410) 385-3700

Counsel for Plaintiff Ohana Growth Partners, LLC

Exhibit 10F

From:	Ryan Wagner
To:	Glenn Norris; Justin Drummond
Subject:	Reisterstown Debrief
Start:	Tuesday, July 11, 2023 11:30:00 AM
End:	Tuesday, July 11, 2023 12:00:00 PM
Location:	Microsoft Teams Meeting
Attachments:	image002.png image003.png

Sorry for the late response. This one fell through the cracks in the mix of the other emails.

Does 11:30 AM EST work?

____

Microsoft Teams meeting

Join on your computer, mobile app or room device

Click here to join the meeting <https://teams.microsoft.com/l/meetup-join/19%3ameeting_MjczMDMxZWItZGYzOC00MmY0LTg5Y2QtMDM4ZWZhY2M5NTcw%40thread.v2/0?context=%7b%22Tid%22%3a%2212be282d-af65-44c5-9b03-ca46dc2f46ee%22%2c%22Oid%22%3a%2241aaa976-a65c-4d39-9b99-476c29593ca1%22%7d>

Meeting ID: 216 499 682 957
Passcode: SsDoSc

Download Teams <https://www.microsoft.com/en-us/microsoft-teams/download-app> | Join on the web <https://www.microsoft.com/microsoft-teams/join-a-meeting>

Or call in (audio only)

+1 469-214-8508,,476413323# <tel:+14692148508,,476413323#>   United States, Dallas

Phone Conference ID: 476 413 323#

Find a local number <https://dialin.teams.microsoft.com/d44639be-1769-4cd6-be1f-ae31789b582d?id=476413323> | Reset PIN <https://dialin.teams.microsoft.com/usp/pstnconferencing>

Learn More <https://aka.ms/JoinTeamsMeeting> | Meeting options <https://teams.microsoft.com/meetingOptions/?organizerId=41aaa976-a65c-4d39-9b99-476c29593ca1&tenantId=12be282d-af65-44c5-9b03-ca46dc2f46ee&threadId=19_meeting_MjczMDMxZWItZGYzOC00MmY0LTg5Y2QtMDM4ZWZhY2M5NTcw@thread.v2&messageId=0&language=en-US>

____

____

From: Glenn Norris <glenn@ohanagp.com <mailto:glenn@ohanagp.com> >
Sent: Monday, July 10, 2023 4:17 PM
To: Justin Drummond <Justin.Drummond@ohanagp.com <mailto:Justin.Drummond@ohanagp.com> >; Ryan Wagner <Ryan.Wagner@ohanagp.com <mailto:Ryan.Wagner@ohanagp.com> >
Subject: RE: Reisterstown Debrief

Yes, how about tomorrow or Wednesday around 11 either day.

Glenn Norris

Chief Financial Officer
Ohana Growth Partners, LLC

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd

Exhibit 10F

Timonium, MD 21093

www.planetfitness.com <http://www.planetfitness.com/>

“Culture eats strategy for breakfast”

From: Justin Drummond <Justin.Drummond@ohanagp.com <mailto:Justin.Drummond@ohanagp.com> >
Sent: Monday, July 10, 2023 3:20 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com <mailto:Ryan.Wagner@ohanagp.com> >; Glenn Norris <glenn@ohanagp.com <mailto:glenn@ohanagp.com> >
Subject: RE: Reisterstown Debrief

Thanks for the note.

Are all of us, including JB, syncing up one day soon to chat about build expectations?

Thank you.

Justin Drummond

Chief Operating Officer
Ohana Growth Partners, LLC

office 410-252-8058 x214
212 W. Padonia Rd
Timonium, MD 21093

www.planetfitness.com <http://www.planetfitness.com/>

“Culture eats strategy for breakfast”

From: Ryan Wagner <Ryan.Wagner@ohanagp.com <mailto:Ryan.Wagner@ohanagp.com> >
Sent: Friday, July 7, 2023 6:36 PM
To: Glenn Norris <glenn@ohanagp.com <mailto:glenn@ohanagp.com> >; Justin Drummond <Justin.Drummond@ohanagp.com <mailto:Justin.Drummond@ohanagp.com> >
Subject: Reisterstown Debrief

To state the obvious

* Development is responsible for building our product, which is our clubs.
* Building a club requires a waterfall project management methodology, which means the project goes from start to finish as planned without modifications.
* Ensuring the project is completed as planned, on time, and budget is critical to our success.
* The above is equally valid for remodels and re-equips.

Until recently, I thought the following was also equally obvious:

* PCI compliance - If billing data/transactions are involved, they must adhere to PCI compliance requirements.
* Fire Alarm Functionality – If we are open to the public, we should take appropriate action to ensure the system works properly.

Reason for today’s Visit:

* Merlowe was there in response to the Fire Alarm System going off “non-stop.”
* I was there to follow up on a problem brought to my attention by SES and our SOC about the SES/HVAC system.
* We agreed to go together so that I could share my insights on connectivity and she could share her insights on HVAC.

Penalties/Risks for not adhering to PCI Compliance include:

* Fines and Penalties
* Increased Audit and Assessments
* Damage to the PF Brand
* Suspension/Termination of Processing Privileges

Exhibit 10F

* Lawsuits and Other Legal Consequences

I have already confirmed that we were operating outside of PCI compliance. The time and materials it took Marc to bring us back into PCI compliance appear to have been less than an hour of labor and less than 20$ of materials. He may say the material cost was more, but I will point out that part of his work put our PCI compliance in a risky state, and during the post-work follow-up, we removed that risk. Thus reducing the total material cost.

Penalties/Risks for Operating without a Functioning Alarm System:

(Unlike PCI Compliance – I am not an expert on Fire Alarm Systems and rely on publicly available information.)

* Injury or Death
* Fines, Penalties, and Closure of the Business

* It seems pretty consistent that most jurisdictions state that operating a business without a functioning fire alarm system is illegal, particularly with open to the public.

* Lawsuits and Other Liabilities
* Voided Insurance Policies or Refusal to Cover Related Damages
* Damage to the PF Brand

Merlowe told me that the system has been alerting and notifying her “non-stop” for quite a while. Merlowe and I Reviewed the Fire Alarm System logs, which showed alternating NAC 1 and NAC 2 fault codes at a frequency that matches her description of “non-stop.” Googling that code, I can see that the NAC is Notification Application Circuit, and the many diagnostic guides indicate that this comes from a cut, broken, damaged, or loose wire connecting the annunciator to the horns, bells, speakers, strobe lights, etc. This part of the system would notify people of a problem and save lives. Merlowe said the annunciator is a new part of the system installed in this remodel. The fault error alone is not enough to determine if the system would or would not function properly. However, all reference points state that a qualified fire alarm technician should address the NAC fault as quickly as possible to ensure the safety of all building occupants.

One thing that stood out to me, is that the Fire Alarm System faults were constant for days – or longer. We stopped scrolling through the logs after a couple days of it being the exact same faults repeatedly. Per the logs, the faults stopped right before I arrived. Merlowe only walked into the club a little bit before I did, and neither of us told anyone to do anything. I never said anything about why I was there, and I believe Merlowe only said she was there to check on the Fire Alarm System. How did they know what the issue was, and how did they “fix” it so quickly? If it was such an easy and quick fix, why did they let it go on for so long and were we at risk the entire time?

Ryan Wagner

Vice President of IT
Ohana Growth Partners, LLC

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093

www.planetfitness.com <http://www.planetfitness.com/>

“Culture eats strategy for breakfast”

Exhibit 10K

From:	Ryan Wagner
To:	Glenn Norris
Subject:	RE: Recap from meeting with Josh Beyer this morning
Date:	Friday, September 1, 2023 5:02:47 PM
Attachments:	image001.png ohanagrowthpartnersfinallogo_7fa8dba2-2909-40ee-839a-12ba06da3de6.png v4.0.zip

Yes, sorry for the gap - it has been go-go-go non-stop all day.

The meeting is at 8:30 am

The established plan:

- We meet every Friday morning. Just the two of us for the first month to sync and align. Then bring in who we need to for further progress.

Josh Ask:

- How does he know things are being done and on time.
    - We reviewed the existing checklist and he said that was great and exactly what he needed. He acknowledged that he has never seen Andrew present this at any meeting and he is committed to making sure he has an updated checklist from Andrew by Monday morning.
    - I followed up with that to provide him an updated checklist that broke out items better and enhanced the when column with context to help everyone understand what and when.

I highlighted a few key parts of the document that address issues that need to be addressed before we have an approved floor plan and critical issues that might seem innocuous may have significant risks for us by not doing it.

- We don’t use this or that type of cable because… they can cause fires or release toxic gas
- We need the server room to be within a specified distance to drop points like the server room because… the cable can’t transmit further and it causes network issues.
- We need to use grommets at certain times because… it will keep the cable from being damaged and require replacement and can prevent other risks
- We need to be mindful of how close low-volt cables are to electrical conduits because… the electrical conduits can cause network/internet issues

We discussed key times when PFHQ requires things to be done:

- Ordering of required hardware
- Compliance Forms
- Physical Pre-Sales Sites required geotagged photos submitted when OSI or other non PFHQ certified vendors do the work
- Pre-Open certification when OST or other non PFHQ certified vendors are doing the installation

We discussed how the first two take less than 5 minutes of combined effort and how in my opinion if that isn’t being done, and HQ is getting on us about it, then we shouldn’t assume the harder stuff is

Exhibit 10K

being done. He agreed.

He said that he understands that this was only an extremely small portion of the issues and we will need the time to go through it in small bite size chunks. We will be walking Takoma Park as it approaches the open date and we will go through the 15 page document item by item so he can see how little is done to meet requirements and standards. Even the little part we did cover, he appeared to understand this really is the tip of the iceberg and he understands those whys better now.

He said that Bill and the rest don't need to understand the why, only that we are doing it. I didn't take that as a hiding thing from them, but rather a "no bill – you can't decide what is important. It must be done even if you don't understand it or the why".

He wanted to push for Andrew to do 100% including adding assets into Woven. I said that I would prefer to have the Help Desk onboard the equipment for two reasons. One I know it will be done correctly, and I also know that it's very time consuming for anyone to learn how to do it right. The example I gave is "you can't put ZV for the name of the ZeeVee Modulator – you have to put in ZeeVee or else we end up having to redo it later anyway" I said that if Andrew can get the checklist done every week and is meeting the standards which includes a much easier task of taking picture of the equipment plate that has a serial number then I have no problem talking about it being added at a later time. He agreed.

Final thing, Since the checklist was updated. I replaced the old standards document to use the reference document that you saw because It is much easier for someone to see in black what PFHQ says and then in red how we have chosen to meet that. It has all the necessary information for Andrew and everyone that has looked at it, which includes a few people who are part of the team that writes the PFHQ standards document, says that it's amazing and have asked for a copy to use and show others.

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Friday, September 1, 2023 4:09 PM

Exhibit 10K

To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Subject: Recap from meeting with Josh Beyer this morning

Ryan, do you have a recap to share with me from your meeting with Josh Beyer this morning?

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Thursday, August 31, 2023 4:01 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Glenn Norris <glenn@ohanagp.com>
Subject: FW: meeting at 2PM tomorrow- agenda items to discuss

Good meeting, thank you. See some notes below in red to make sure you follow up on with me.

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Wednesday, August 30, 2023 3:37 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Glenn Norris <glenn@ohanagp.com>

Exhibit 10K

Subject: meeting at 2PM tomorrow- agenda items to discuss

Ryan, this is our agenda tomorrow.

1. Goals for September-discuss and make sure we agree on the execution timing
    a. Fire and Hire – send me the job description & KPI-send me the updated JD and KPI by 9-15.
    b. Access for all users is one log on only per person, ease to log on and easier access to a consistent cloud files format. Communicate and Trial it before a blanket install
    c. Meet with Josh Beyer(one on one) each week for 30 minutes to an hour to align IT and Development. Send an email to me post meeting from both of you on the topics discussed and issues resolved. When is that meeting time and day-(Friday at 830) ? Tomorrow's meeting- goal is to be in total compliance when a project is deemed complete/open for business……..discuss who will be the doer's and accountable parties ………the accountable parties must work as one to make sure the doer's see a unified front. Being in every meeting for IT is critical from planning to finish. Build Trust in each other- no non-verbals or verbals that belittle others during meetings to recap project status and in a Green, Yellow or Red mode.
2. IT Budget to Actual through July 31, 2023 for each company. Next Tuesday at 1PM
3. Cielo update on what they still have in our cash……….show me the projects they will work on to get it to Zero by 12-31 or how they will still owe a balance and pay us that balance that is anticipated by 9-30-23. Need update on status by Monday.
4. Comcast Double billing update. Is it resolved? If not, why? Need a plan to get all $$ returned by 9-30-23. Need update on status by Monday.
5. Using Monday.com in the interim for Development/IT projects…………hire someone that can manage this and attend development meetings. Refer to 1c.
6. Discuss the replacement of Andrew Dinh with Josh Beyer – what must Andrew do by 9-30-23 to prevent this replacement from occurring.
7. Timeline of IT changes and potential budget for those changes to occur- month by month time line through 12-31-24. Must do this with Glenn ahead of any implementation . Need 30 days in advance of any launch.
8. KPI Form- let's review for changes. KPI for August is Sept 14. Let's review for updates.
9. What is your biggest challenge each day? Tell me ???
10. What can I do to help you? Tell me???

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

Exhibit 10K

5 of 5

Exhibit 10P

PLANET FITNESS®

EXHIBIT “K-4”
TO THE DISCLOSURE DOCUMENT

POS AGREEMENTS

Exhibit 10P

ABC FITNESS SOLUTIONS

ABC Fitness Solutions, LLC
P.O. Box 6800
Sherwood AR 72124

abcfitness.com

ABC Club #	PF Group #	RCS Club #

Business Name (dba):	
Authorized Owner/Officer:	Title:

Street Address:		
City:	State:	Zip:
Phone:	Email Address:	

Business Name (legal):	
Federal Tax ID# (TIN or EIN):	Date of Incorporation:
Location of Incorporation:	Type of Business (ie S Corp, LLC, etc.):

BILLING SERVICES AGREEMENT ("Agreement")

This Agreement made on _________________, by and between ABC Fitness Solutions, LLC, a Delaware limited liability company, (hereinafter "ABC") and ____________________________a/an ________________________________("the Client"):

1. Merchant and Bank Account Set-up: Client hereby appoints ABC to act as its attorney-in-fact as follows: (i) to establish and maintain a credit card processing merchant agreement and an ACH processing agreement on Client's behalf with such credit card processor and ACH processor as ABC may designate and which have been approved by Pla-Fit Franchise LLC ("Franchisor") pursuant to Section 11.5 of the Second Amended and Restated Master Services Agreement between Franchisor and ABC dated January 13, 2023 ("MSA") (ii) to receive sales data from Client and tender it to a credit card or ACH processor, for processing/to receive payment due from Client's members under Client membership agreements, as descr bed in Paragraph 2, below ("Periodic Payments"); and (iii) in connection with such merchant account and this Agreement, to execute any and all documents and take any and all other actions, on behalf of Client, that ABC deems necessary or appropriate without further authorization or consent of Client; provided, however, that ABC shall not enter into and has no authority to bind or commit Client to terms for the collection of Periodic Payments which are Inconsistent with the MSA and this Billing Services Agreement. In addition, ABC shall not enter into minimum term or minimum commitment arrangements in relation to Periodic Payments that would preclude Client from terminating such arrangements with or without cause and for no penalty. For purposes of this Agreement, the terms "**Inconsistent**" and "**Inconsistency**") as used in this Billing Services Agreement shall mean any term which (i) is not in agreement with, not compatible with or at variance with a term of the MSA and/or this Billing Services Agreement (ii) would add new or additional material obligations on Client, other than those specifically set forth in the MSA and this Billing Services Agreement; or (iii) would limit, remove or prevent Client from exercising a material right, remedy or benefit available to Client under the MSA and this Billing Services Agreement. ABC currently has credit card processing relationships WorldPay and ACH processing arrangements in place with Regions Bank. ABC agrees to notify the Client of any additional processors that it may utilize in connection with the processing of the Client's credit card and ACH transactions. The services provided by ABC and its vendors under this Agreement are "Services" for purposes of the MSA and subject to the terms of the MSA. In particular, ABC shall ensure that its agreements with its processors require the processors to comply with the provisions of Sections 11 and 17 of the MSA and with the terms of Section 18 (as those terms existed under the First Amended and Restated Master Services Agreement between ABC and Franchisor).

2. ABC agrees to bill, service and account for all acceptable membership agreements of the Client that have been delivered to ABC from time to time under this Agreement. Upon receipt of an acceptable membership agreement and such membership agreement becomes an active account, ABC will maintain appropriate account information during the time ABC is actively collecting the account on behalf of the Client. For purposes of this Agreement, an "acceptable membership" will satisfy the following minimum conditions: include the member's first and last name and billing information, have been approved by the Client via the queue process (if the client is using the approval queue), member's e-mail (if member sign-up is conducted online) and shall not be in default or past due. Where a member has remitted payment to ABC, member's payment obligation to Client in relation to such payment shall be extinguished and client shall not attempt to hold member liable for ABC's nonremittance to Client.

3. The Client agrees to pay ABC for billing services consistent with the attached proposal. Supplier may increase the fees herein, as permitted herein and/or the MSA. All ABC fees will be deducted and retained by ABC from the amount collected on behalf of the Client. The fees apply to all payments on active membership agreements under service by ABC, whether payments are made to ABC or directly to the Client. Fees may be disputed by Client in accordance with Section 4.

4. Billing cycles will occur twice per month. The 1st through the 15th shall represent one billing cycle, while the 16th through the end of the month shall represent the other billing cycle. Net receipts for each billing cycle will be remitted to the Client by the 5th business day following the cycle cutoff. ABC will not be responsible for delay in remittance due to weekends, holidays or other conditions beyond the reasonable control of ABC. Net receipts are equal to the total membership agreement payments less the sum of the following: (I) reversals, charge backs, refunds or other credits against payments collected; (II) the billing fee set forth in paragraph

Exhibit 10P

3; (III) any credit for payments made directly to the Client; (IV) amounts owing to Franchisor; and (V) any service or late charge, cancellation fee, or other charge or amount due from Client to ABC pursuant to this Agreement, or any other agreement between Client and ABC or any policy established by ABC from time to time. Client may also request an early deposit of Available Collected Funds any business day of the month. Available Collected funds shall mean the amount of funds actually collected and received by ABC from members on behalf of Client pursuant to membership agreements, or any other agreement serviced by ABC under this Billing Service Agreement, net of ABC's projected billing fees and applicable administrative fees for such early deposit and net of projected charge backs and refunds. ABC will use its reasonable best efforts to post Available Collected Funds to Client's account one business day after their actual receipt. No later than end of month, ABC will provide Client with a reconciliation statement setting for in reasonable detail the gross total membership agreement payments and the amount of and nature of any deductions from such gross amount ("Reconciliation Statement"). Client may dispute in good faith any deduction from the membership agreement payments by notifying ABC in writing and describing, in reasonable detail, the basis for such dispute. Client and ABC shall diligently pursue an expedited resolution of such dispute. If Client fails to dispute a Reconciliation Statement within ninety (90) days of receipt it shall be deemed to have waived its right to dispute the Reconciliation Statement.

5. Only current membership agreements will be acceptable membership agreements under this Agreement. If, in the sole discretion of ABC, a past due account becomes uncollectible, the Client will be responsible for further collection of said account and ABC shall be released from any further responsibility with respect to such membership agreement.

6. The Client may cancel the membership agreement of any member, and such membership agreement will be removed from the active list and the Client will be notified. Cancellations will not be accepted from individual members, only from the Client itself, unless prior authorization is received from Client.

7. Either party may cancel this Agreement by giving the other party ninety (90) days written notice. In addition, if the Client is not in default with respect to any obligations it owes to ABC or its affiliates under this or any other Agreement, it may unilaterally convert the service provided by ABC from "Full Service" to "Processing Plus" by providing at least thirty (30) days prior written notice to ABC. ABC shall provide such "Processing Plus" service for the cost and with the benefits generally applicable to customers of comparable size as the Client.

8. The Client shall pay any and all federal, state or local excise, sales or use taxes or similar taxes imposed in respect to all membership agreements serviced by ABC for the Client under this Agreement, or the services involved with respect to such membership agreements ("Taxes"), and complete and file all required tax reports related thereto, all in a timely manner, and hereby agrees to indemnify and hold ABC, its officers, directors, shareholders and employees harmless from any loss, including attorneys' fees, resulting from its failure to do so.

9. If ABC is required to withhold or pay any of the foregoing said Taxes, or if the Client ever becomes liable to ABC for any sums or losses, the amount so paid by ABC for said Taxes and any sums expended or losses incurred by ABC for which the Client is responsible to indemnify ABC, will be deducted from all money collected, held or controlled by ABC under any existing agreements between ABC and the Client, including, but not limited to, this Agreement and any billing and/or collection agreements, and further including, but not limited to, any such money held in any account or accounts of the Client held or set up by ABC related to same, as well as from any collections and/or funds held or controlled by ABC for the benefit of the Client related to same. In the event the amounts are not satisfied, any remaining amounts owed will be due and payable to ABC by the Client within three (3) of receipt of ABC's written notice of the claim and request for payment to the Client by ABC.

10. The Client hereby agrees to indemnify, defend and hold ABC, its officers, directors, shareholders, agents, contractors and employees harmless from any liability, claim, loss and expense, including attorneys' fees, resulting from its failure to perform its obligations in this Agreement or from its actions or omissions in connection with the operation of its club facilities, including, without limit, the failure to comply with any applicable federal, state or local laws, rules, regulations or ordinances. ABC shall defend, indemnify and hold Client, its affiliates, clients and their respective officers, directors, shareholders, members, managers, partners, legal representatives, successors and assigns (the "Client Group") harmless of, from and against any and all claims, losses, demands, damages, actions, suits, liabilities, fines, penalties, settlements and expenses, including attorneys' fees and litigation costs (collectively "Claims"), whether direct or indirect, incidental, consequential, or otherwise, arising out of or relating to: (a) any claim of violation of any federal "no call" list or the Telephone Consumer Protection Act or failure to comply with any other applicable federal laws, rules or regulations or any state or local laws, rules, regulations or ordinances, (b) ABC's breach, default or failure to comply with any terms of this Agreement, or any other agreement between ABC and Client, and (c) ABC's negligence or intentional misconduct but excluding any liability for Claims arising out of or caused solely by the Client Group's own breach of the Agreement or any applicable law or its own negligence or intentional misconduct. Client agrees that if it becomes aware of any potential violation of any applicable law by ABC, it shall promptly notify ABC in writing. The foregoing provision shall not obligate Client to conduct any affirmative research into ABC's compliance with such laws but only to notify ABC of non-compliance of which it becomes aware in the ordinary conduct of its business.

11. This Agreement shall be governed by the laws of the state of New Hampshire. Any litigation brought hereunder shall be brought only in a state or federal court of general jurisdiction in Pulaski County, Arkansas.

12. By executing this Agreement, the undersigned agrees to be bound by the Addendum to Billing Services Agreement attached hereto and incorporated herein by this reference.

Exhibit 10P

Executed this ________day of ___________________________, _______________.

(Printed Name} **X__________________________________** ***(Signature)*** **ABC Fitness Solutions, LLC** **208 E. Kiehl Avenue** **Sherwood, AR, USA 72120**	**X____** ***(Printed Name)*** **X____** ***(Signature)*** **Corporation Owner or Agent**

Exhibit 10P

ADDENDUM TO BILLING SERVICES AGREEMENT

WHEREAS, ABC and Client entered into a Billing Services Agreement attached hereto (the "BSA") pursuant to which Client agreed to be bound by the terms of this Addendum which are incorporated into the BSA;

WHEREAS, ABC has entered into an agreement with Worldpay, LLC (“Worldpay”) governing acceptance of credit and debit card transactions initiated by Client which obligates it to obtain Client's agreement to abide by certain rules and regulations promulgated by Worldpay;

WHEREAS, the Client will receive substantial benefit and gain as a result of its members being able to make payments for Client services via credit and debit cards and therefore is willing to be bound by the rules and regulations as described herein; and

WHEREAS, all capitalized terms used herein but not otherwise defined shall have the meaning given to them in the BSA or the Operating Regulations (as defined below).

NOW, THEREFORE, in exchange for good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, Client agrees that the by-laws, operating regulations and/or all other rules, policies and procedures, including but not limited to the Payment Card Industry Data Security Standards, the VISA Cardholder Information Security Program, the Mastercard Site Data Protection Program and any other program or requirement (collectively, the Operating Regulations”) that may be published and/or mandated by Mastercard International Inc., VISA U.S.A. Inc., Discover and certain similar entities (collectively, the “Associations”) are incorporated by reference into this Addendum and that nothing in this Addendum shall be construed to interfere with or lessen the right of ABC, Worldpay’s designated Member Bank, or the Associations to terminate the BSA at any time. In the event of a conflict between this Addendum and the Operating Regulations, the Operating Regulations will control.

A. Client acknowledges and agrees:

a. it is responsible for the actions of its employees and agents;

b. it will comply with all applicable laws and regulations and all applicable parts of the Operating Regulations; including those parts regarding the ownership and use of Association Marks;

c. ABC or an Association is authorized to research Client’s background including, but not limited to, credit background checks, banking relationships, and its financial history;

d. notwithstanding any provisions in the agreement to the contrary, information obtained in

Exhibit 10P

connection with Client's application or processing relationship may be shared with Association for any legitimate purpose;

e. it will notify ABC of any 3rd party that will have access to cardholder data;

f. it will comply with, and will contractually require its suppliers and agents to comply with, the provisions of the Cardholder Information Security Program (CISP) and PCI DSS, or other security program as required by an Association and demonstration compliance with these security obligations; and

g. Associations may conduct, or direct another party to conduct, an audit of Client at any time, and Client must comply in all material respects with such audit until its completion.

B. Client represents and warrants that it will not:

a. discriminate against Cards or Issuers (e.g limited acceptance options) except in full compliance with the Operating Regulations;

b. intermingle fees associated with an Associations' transactions with fees associated with other Card transactions in its pricing;

c. submit any transaction to ABC that was previously charged back and subsequently returned to the Client, irrespective of Cardholder approval;

d. knowingly submit any transaction that is illegal or that the Client should have known was illegal. Client acknowledges that such transaction must be legal in both Cardholder's and Client's jurisdiction;

e. submit a transaction that it knows, or should have known is either fraudulent or not authorized by the Cardholder;

f. require a Cardholder to complete a postcard or similar device that includes the Cardholder's account number, Card expiration date, signature, or any other Card account data in plain view when mailed, nor request a Card Verification Value 2 ("CVV2") for a card-present transaction, nor retain or store any portion of the magnetic-stripe data subsequent to the authorization of a sales transaction, nor any other data prohibited by the Operating Regulations or this Addendum, including CVV2;

g. add a surcharge to transactions, except as expressly permitted by, and in full compliance with, the Operating Regulations;

h. charge a minimum or maximum amount for a transaction unless expressly authorized by, and in full compliance with, the Operating Regulations;

i. disburse funds in the form of cash unless Client is participating in full compliance with a program supported by an Association for such cash disbursements and in full compliance with the Operating Regulations;

j. submit a transaction that does not result from an act between the Cardholder and the Client;

Exhibit 10P

k. accept a Card issued by a U.S. Issuer to collect or refinance an existing debt, unless expressly authorized by, and in full compliance with, Operating Regulations;

l. request or use a Card account number for any purpose other than as payment for its goods or services; and

m. add any tax to transactions, unless applicable law expressly requires that a Client be permitted to impose a tax. In such event, any tax amount, if allowed, must be included in the transaction amount and not collected separately."

c. Applicable to ABC Clients participating in the American Express OptBlue Program. The following will only apply to Client's participation in the American Express Program, as controlled by the American Express OptBlue Program Operating Regulations. (Capitalized terms below are defined in the American Express Operating Guide or the American Express OptBlue Program Operating Regulations):

a. Client must comply with, and accept Cards in accordance with, the terms of its BSA and the American Express Merchant Operating Guide, as such terms may be amended from time to time.

b. Client acknowledges that the American Express Merchant Operating Guide is incorporated by reference into this Agreement (and is available online at the following web link: https://icm.aexp-static.com/content/dam/gms/en_us/optblue/us-mog.pdf).

c. Client expressly authorizes ABC to submit transactions to, and receive settlement from, American Express on behalf of the Client.

d. Client expressly consents (i) to ABC collecting and disclosing Transaction Data, Client Data, and other information about the Client to American Express; and (ii) to American Express using such information to perform its responsibilities in connection with the Program, promote the American Express Network, perform analytics and create reports, and for any other lawful business purposes, including commercial marketing communication purposes within the parameters of the Program Agreement, and important transactional or relationship communications from American Express.

e. Client acknowledges that:

□ By checking this box, Client opts out of receiving future commercial marketing communications from American Express.

Client may continue to receive marketing communications, however, while American Express updates its records to reflect this choice. Opting out of commercial marketing communications will not preclude you from receiving important transactional or relationship messages from American Express.

Exhibit 10P

f. Client acknowledges that it may be converted from the Program to a direct Card acceptance relationship with American Express if and when it becomes a High CV Merchant in accordance with Section 10.5, "High CV Merchant Conversions”

o Client expressly agrees that, upon conversion, (i) Client will be bound by American Express' then-current Card Acceptance Agreement; and (ii) American Express will set pricing and other fees payable by the Client for Card acceptance.

g. Client acknowledges that American Express may use information obtained in the Client application at the time of setup to screen, communicate, and/or monitor Client in connection with Card marketing and administrative purposes.

h. Client agrees that it shall not assign to any third party any payments due to it under its respective BSA, and further agrees that all indebtedness arising from Charges will be for bona fide sales of goods and services (or both) at its Establishments and free of liens, claims, and encumbrances other than ordinary sales taxes; provided, however, that the Client may sell and assign future Transaction receivables to ABC, its affiliated entities and/ or any other cash advance funding source that partners with ABC or its affiliated entities, without consent of American Express.

i. Client agrees that American Express is a third-party beneficiary to the BSA and retains all rights, but not obligations, in the BSA that will fully provide American Express with the ability to enforce the terms of the BSA against the Client.

j. Client may opt out of accepting Cards at any time without directly or indirectly affecting its rights to accept Other Payment Products.

k. Client agrees that ABC may terminate the Client's right to accept Cards if Client breaches any of the provisions in this Section or the American Express Merchant Operating Guide.

l. Client agrees that ABC has the right to immediately terminate a Client for cause or fraudulent or other activity, or upon American Express' request.

m. Client agrees that its refund policies for purchases on a Card must be at least as favorable as its refund policy for purchases on any Other Payment Products, and further agrees that the refund policy be disclosed to Cardmembers at the time of purchase and in compliance with Applicable Law.

n. Client acknowledges that it is prohibited against billing or collecting from any Cardmember for any purchase or payment on the Card unless Chargeback has been exercised, the Client has fully paid for such Charge, and it otherwise has the right to do so.

o. Client agrees it must comply with all Applicable Laws, rules and regulations relating to the

Exhibit 10P

conduct of the Client's business, including the DSR and PCI DSS, each as described in Chapter 15, "Data Security."

p. Client agrees that it will report all instances of a Data Incident immediately to ABC after discovery of the incident.

q. Client agrees it will cease all use of, and remove American Express Licensed Marks from the Client's website and wherever else they are displayed upon termination of the ABC BSA or a Client's participation in the Program.

r. Client will ensure data quality and agrees that Transaction Data and customer information will be processed promptly, accurately and completely, and will comply with the American Express Technical Specifications.

s. Client agrees it is solely responsible for being aware of and adhering to privacy and data protection laws and provide specific and adequate disclosures to Cardmembers of collection, use, and processing of personal data.

Except as specifically stated in this Addendum, the BSA shall remain in full force and effect.

Exhibit 10P

Planet Fitness Full Service Billing Proposal

Goods and Services	Fees
English and Non-English versions of DataTrak/IGNITE Software Fee include unlimited software access and technical support as it is described in the Agreement. Technical support will be provided on a 24/7 basis in English and M-F 8am to 5pm Central Time in Spanish (or other language as mutually agreed), training, all software upgrades, unlimited users, members and inventory items, and member emails and texts.	**ENGLISH-ONLY VERSION:** $[redacted] per Service Recipient (Club Location) per Month. As of February 1, 2023, the above pricing shall automatically be increased to $[redacted] per Service Recipient (Club Location) per month NON-ENGLISH VERSIONS An additional fee of $[redacted] USD for each NON-ENGLISH version per Service Recipient (Club Location) per Month. For example, a Service Recipient using the SPANISH and FRENCH versions of Data Trak will pay $[redacted] per location (ENGLISH-ONLY $[redacted] plus SPANISH $[redacted] plus FRENCH [redacted] = $[redacted])
ABC Professional Endpoint Services (ABCPES) fee ABCPES includes: • Daily computer maintenance • Password recovery o Supplier can reset the staff password if needed. o Supplier can also control all administrator passwords. • URL/DNS whitelisting (Internet blocking) • Windows Update management • Remote monitoring & Audits o Remote Monitoring ▪ Alerts setup for the following sections • Health of computer • Online/Offline status of computer • Virus alerts ▪ Audit • Supplier audits all offline computers on a quarterly basis to determine why offline. • Virus removal and repair o Supplier will try to repair any damage done by a virus or work with the AE on other options. • Anti-Virus o Provide Webroot Antivirus (or comparable product) to all Customer POS computers	$[redacted] per Standard Workstation per month (in excess of two (2) Standard Workstations)
Applies only to Dues Billing Transactions EFT/ACH/Savings Bank Drafts	$[redacted] per Transaction.
Applies only to Dues Billing Transactions Credit Card Drafts	$[redacted] per Attempted Invoice

Exhibit 10P

Goods and Services	Fees
Dues Billing and Club Account	Fees for settled credit card transactions: Visa: MC, Discover [redacted] Amex: [redacted] [redacted] decline fee for any processed card transaction which is declined
POS Credit Card Transactions (real-time: card present & card-on-file)	Actual Costs passed through from processors. Additional based on payment activity: [redacted] per authorization attempt [redacted] settled sales [redacted] per monthly service fee [redacted] per Chargeback fee [redacted] per Retrieval fee [redacted] per batch fee [redacted] per T&E transaction Such other fees as may be set forth on the Service Recipient's Merchant Agreement (or agreed upon successor/replacement agreement).
Dues Billing and Club Account Billing Deposits	Billing Deposits: Same day wire fee: [redacted] per deposit 24-hour ACH fee: [redacted] per deposit Unlimited ACH Daily Billing Deposits: Flat Monthly fee: [redacted]
PCI Compliance (currently Viking Cloud) Fee	[redacted] per Month per Service Recipient (club location)
ACH Return Fee	[redacted] per ACH Return
Point-to-Point Encryption service	[redacted] per month per terminal.
Full Service Program	[redacted] per email per inbound or outbound text per outbound call + postage per letter per inbound call answered by Agent
Web Join fee	[redacted] or as otherwise specified by Customer's Methods of Operations
Supplier provided in-person, onsite training	[redacted] per trainer per day. One (1) day minimum per site visited.
Contract Storage Fees for Paid in Full Memberships	[redacted] per contract per month
ACH Unauthorized Returns	[redacted] per return

Exhibit 10P

Goods and Services	Fees
Attempted recovery of chargeback	[redacted] per chargeback
Sales Tax Calculation (Avalara) Fee	[redacted] per club per month This service is enabled as part of conversion to Ignite and is not chargeable until the Service Recipient upgrades.
Contract Autorenewal Notification Service	[redacted] + postage per letter This service is enabled for those only Service Recipient Locations in states that require member notification prior to contract autorenewal.

Accepted by:

Group Number

Owner's Signature

Date

Exhibit 10P

Merchant Agreement

ABC FITNESS SOLUTIONS

Central Bank

7707 Forsyth Blvd • St. Louis, MO 63105
Phone 1-800-697-0480

Agent Code		MCC		Date
Provide any existing MIDs on TSS		TID #		MID #
Legal Business Name *(Required)*				
Merchant Name *(DBA)*				
Federal Tax ID # *(Required)*		Taxable State *(Required)*		
Legal Business Address				
City	State	Zip	Phone #	Fax #
Mailing Address *(if different than Legal Business Address)*				
City	State	Zip	Phone #	Fax #
Location Address				
City	State	Zip	Phone #	Fax #
Web address *(list all URLs used; attach separate sheet if necessary)*				
Email address *(Required)*			Delivery method of month-end Merchant Statement ☐ Letter ☒ Email	

Special Fee Conditions See Section 3.24 of the terms & conditions for a full description of fees.

No SSL Authorization Surcharge; No Minimum Monthly Fee or Cancellation Fee; Mid Chain 219891; combined ACH required; AMEX Direct

Important Information about Procedures for Opening a New Account

To help the government fight the funding of terrorism and money laundering activities, Federal law requires all financial institutions to obtain, verify, and record information that identifies each person who opens an account. ***What this means for you:*** When you open an account, we will ask for your name, address, date of birth, and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents.

Merchant Acceptance/Bank Disclosure

Each person signing below 1) agrees that they have received a copy of the terms and conditions [T & C pages 1–7] associated with this agreement, 2) agrees to all such terms and conditions, 3) agrees that all information provided on this agreement is true, correct, and complete, 4) agrees that they have the legal power and authority to execute this agreement, 5) authorizes the Acquirer to investigate, either through its own agents or through credit bureaus, all information provided in this agreement and on the individual(s) listed on this agreement, 6) agrees that Acquirer may give information to others, including creditors and credit reporting agencies, concerning the Acquirer experience with merchant, and that 7) Acquirer may request additional information as needed. **Member Bank (Acquirer) Information:** Central Bank of St. Louis, 7707 Forsyth Blvd, St. Louis, MO 63105 • Phone 1-800-697-0480.

Important Acquirer Responsibilities

1. Central Bank is the only entity approved to extend acceptance of the Payment Card Brands products directly to a Merchant.
2. Central Bank is responsible for educating Merchants on pertinent Payment Card Brands Operating Regulations with which Merchants must comply.
3. Central Bank, not the ISO, must hold, administer and control all reserve funds derived from settlement.
4. Central Bank, not the ISO, must hold, administer and control settlement funds for the Merchant.
5. Central Bank must be a principal (signer) to the Merchant Agreement.

Important Merchant Responsibilities

1. Complying with cardholder data security and storage requirements.
2. Maintaining fraud and chargebacks below established thresholds.
3. Reviewing and understanding the Merchant Agreement.
4. Complying with the Payment Card Brands operating regulations.

The responsibilities listed above do not supersede terms of the Merchant Agreement including the terms and conditions which are provided to ensure the Merchant understands some important obligations of each party and that the Payment Card Brands Member—Central Bank of St. Louis—is the ultimate authority should the Merchant have any problems.

X ______________________________
Signature of Owner, Authorized Officer Print name Title Date

X ______________________________
Signature of Owner, Authorized Officer Print name Title Date

X ______________________________
Signature of Repay Authorized Officer Print name Title Date

X ______________________________
Signature of Acquirer Authorized Officer Print name Title Date

March 14, 2023 **PR APPROVED:**

Exhibit 10P

Merchant Information

Have you been placed on the Combined Terminated Merchant File? □ Yes □ No

Product/Service offered *(restaurant, clothing, auto, etc)* Health and Fitness

Merchant Business Structure

□ C-Corp *(Privately owned)*, State of Inc.________ □ S-Corp *(Privately owned)* □ Partnership *(Privately owned)* □ Sole Proprietor ☒ LLC □ Not for Profit

□ C-Corp *(Publicly owned)*, State of Inc.________ □ S-Corp *(Publicly owned)* □ Partnership *(Publicly owned)* □ Government Agency

Stock symbol, if the merchant is a publicly held company __________

Length of time in business? Years ________ Months ________ Length of time legal entity in business? Years ________ Months ________

Name of previous Visa/MC/Discover®/American Express® processor or bank *(attach 3 current months processor statements):*

Processing Volume *(for internal use only)*

☒ Monthly □ Daily Average Ticket $__________ Maximum Ticket $__________

Monthly Visa/MasterCard/Discover Volume $__________ Monthly American Express Volume $__________

Peak Season Visa/MasterCard/Discover/American Express Volume $__________

Method of Acceptance *(totals must equal 100%)*

Swiped__________% Imprinted__________% MO/TO__________% Internet__________%

Responsible Individual ______% of ownership *(Social Security # or Date of Birth is required if the merchant processes American Express)*

Last name First name MI Title *(Required)*

Residence address City State Zip

Residence phone Social Security # Date of Birth Driver's license # State

First Beneficial Owner ______% of ownership

Last name First name MI Title

Residence address City State Zip

Residence phone Social Security # *(Required)* Date of Birth Driver's license # State

Second Beneficial Owner ______% of ownership

Last name First name MI Title

Residence address City State Zip

Residence phone Social Security # *(Required)* Date of Birth Driver's license # State

Third Beneficial Owner ______% of ownership

Last name First name MI Title

Residence address City State Zip

Residence phone Social Security # *(Required)* Date of Birth Driver's license # State

Fourth Beneficial Owner ______% of ownership

Last name First name MI Title

Residence address City State Zip

Residence phone Social Security # *(Required)* Date of Birth Driver's license # State

Trade References

1) Name/Contact Phone

2) Name/Contact Phone

March 14, 2023

PR APPROVED:

Exhibit 10P

Terminal Information

☐ Global ☐ TSYS ☒ Retail ☐ Restaurant (no tip) ☐ Restaurant/Retail Tips (no auto close)

Terminal type ____________ ☐ Dial ☒ IP Printer/Pinpad type ____________

Software/Gateway *(payment application name)* ☐ Virtual ☐ Shopping Cart ABC Fitness Solutions Version ____________

Merchant Site Survey Report *(To be completed by Independent Agent)*

Merchant location: ☒ Store front ☐ Office building ☐ Warehouse ☐ Residence ☐ Other ____________

Merchant: ☐ Owns ☐ Leases building premises Landlord name ____________ Landlord phone # ____________

Yes	No		Yes	No	
☒	☐	Merchant appears to be conducting business as represented in this agreement.	☐	☒	Have you taken pictures inside and outside of the premises?
☒	☐	Merchant is adequately staffed and stocked to do business.	☒	☐	Have you confirmed the identity of the person who signed the contract?
☒	☐	Merchant has posted any business license(s) required to do business.	☒	☐	Have you confirmed the signor as owner/principal of the business?

Comments Merchant Needs 2 Software TIDs

☐ I hereby verify that I have physically inspected the business premises at this address.

☒ I also verify that all information submitted in this agreement is correct to the best of my knowledge and belief.

Inspected by / Sales Rep *(print)* Agent #

X ____________

Signature Date

Electronic Debit/Credit Authorization

Merchant hereby authorizes Bank, or third party in accordance with this agreement, to initiate debit/credit entries to Merchant's deposit account, as indicated below. This authority is to remain in full force and effect until (a) Bank has received written notification from Merchant of its termination, in such a manner as to afford Bank reasonable opportunity to act on it and (b) all obligations of Merchant to Bank that have arisen under this Agreement have been paid in full. This authorization extends, but is not limited, to such entries to this account which concern discount fees, transaction fees, chargebacks, penalties, service fees, return items fees, lease, rental and purchase charges involving Point-of Sale ("POS") and credit card imprint equipment.

A voided check from this account must be attached.

Bank name Name on account

Address City State Zip

Routing # Account # Phone #

You have the option of accepting Visa credit cards, MasterCard credit cards, Discover cards, American Express Cards, credit cards issued by MasterCard signature debit cards (MasterMoney Cards) or Visa signature debit cards (Check Cards). You may elect to accept any or all of these card types for payment. If you do not specifically indicate otherwise, your agreement will be processed to accept ALL Visa, MasterCard, Discover and AXP Card types.

Indicate Visa, MasterCard, Discover, AXP Card or PayPal types NOT to accept: PayPal

☐ By checking this box, Merchant opts out of receiving future commercial marketing communications from American Express.

MO/TO, Internet Questionnaire *(Complete this section only if credit card processing is more than 25% MO/TO, Internet)*

What % of sales are to: Business consumer ________% Individual consumer ________%

Describe your refund policy in detail (attach sheet if necessary): ____________

Method of marketing: ☐ Newspaper/Magazine ☐ TV/Radio ☐ Internet ☐ Direct mail, brochure and/or catalog ☐ Outbound telemarketing sales

Percentage of products sold via: Phone orders ________% Mail/Fax orders ________% Internet orders ________% Other ________%

Who processes the order? ☐ Merchant ☐ Fulfillment center ☐ Consumer ☐ Other ☐ N/A

Who enters credit card information into the processing system? ☐ Merchant ☐ Fulfillment center ☐ Consumer ☐ Other

If credit card information is taken over the internet, is payment system encrypted by SSL or better? ☐ Yes ☐ No

If the Merchant is an e-Commerce Merchant, is a Merchant Certificate utilized? ☐ Yes ☐ No

If Yes, please provide: Merchant Certificate # ____________ Certificate Issuer ____________ Expiration date ____________

Do you own the product/inventory? ☐ Yes ☐ No ☐ N/A Is product stored at your location? ☐ Yes ☐ No ☐ N/A If No, where? ____________

After charge authorization, how long until the product ships? (days) ________ ☐ N/A Who ships the product? ☐ Merchant ☐ Fulfillment center ☐ N/A

Product shipped by? ☐ US Mail ☐ Other ☐ N/A Delivery receipt requested? ☐ Yes ☐ No ☐ N/A

March 14, 2023 **PR APPROVED:**

Exhibit 10P

Corporate Guaranty/Resolution

(Not required on volumes less than $100,000 monthly—except for high risk accounts)

______________________________, the duly elected, qualified and acting ______________________________
Corporate Secretary** Office Title

of ______________________________ , a ______________________________ (the "Merchant Company"), do hereby certify as follows:
Legal Corporate Name of Merchant Company Incorporation Status

The following resolutions were duly adopted by the board of directors / managing member(s) / general partners (circle one) of the Merchant Company WHEREAS, the Merchant Company desires to enter into a Merchant Agreement (the "Merchant Agreement") with Central Bank Corporation, a Missouri industrial loan corporation ("Bank") and TriSource Solutions, LLC. d/b/a REPAY, a Nevada Limited Liability Company ("ISO"). NOW, THEREFORE, BE IT RESOLVED, that the Merchant Agreement by and among the Merchant, Bank and ISO, is hereby approved and adopted in the form pro-vided by ISO, together with such additions, changes or modifications as may be deemed necessary, advisable or appropriate by the officer(s) executing or causing the same to be completed; and RESOLVED FURTHER, that in connection with the Merchant Agreement, the appropriate officer(s) of the Merchant Company is/are hereby authorized to establish (a) an Operating Account into which funds from credit card sales by the Merchant Company will be directed, and (b) if necessary, a Reserve Account into which funds from credit card sales by the Merchant Company may be directed by Bank in accordance with the provisions of the Merchant Agreement; RESOLVED FURTHER, that the Merchant Company hereby grants Bank a security interest in the funds held by the Merchant Company in the Operating Account and Reserve Account, and the appropriate officer(s) of the Merchant Company is/are hereby authorized to execute all documents rea-sonably required by Bank to perfect such security interests; RESOLVED FURTHER, that the appropriate officer(s) of the Merchant Company is/are hereby authorized to enter into such additional agreements, and take such additional actions as may be reasonably required by Bank or ISO in connection with the Merchant Agreement; and RESOLVED FURTHER, that the Secretary / man-aging member / general partner (circle one) of the Merchant Company is hereby authorized to deliver to Bank and to ISO an Incumbency Certificate, (i) identifying the officers of the Merchant and (ii) verifying the signatures of such officers, as well as a copy of these resolutions, certified by the Secretary of the Merchant (or authorized member or partner), and Bank and ISO are here-by authorized to rely on such Incumbency Certificate and certified copy of these resolutions until formally advised by an authorized officer/member/partner of the Merchant in writing of any changes therein, accompanies by a replacement of the Incumbency Certificate.

I hereby certify under penalty of law, that I have the legal power and have been duly authorized by the company applying for a merchant processing account, to execute this agreement on behalf of the company listed on page one of this Merchant Processing Agreement. Each person listed below (an "Officer") (i) holds the office in the Merchant Company indicated opposite his or her name on the date hereof, (ii) the signature appearing opposite his or her name in the Merchant Acceptance section of Agreement, is the genuine signature of each such officer, (iii) each such Officer, acting individually, is authorized to execute and deliver the Merchant Agreement and each of the agreements and documents contemplated by the Merchant Agreement (collectively, the "Transaction Documents") on behalf of the Merchant Company, and (iv) each such Officer, acting individually, is authorized to perform the Merchant Company's obligations under the Transaction Documents on behalf of the Merchant Company:

____
Print name Officer

X ____
Signature

In witness whereof, I have executed this certificate this ________ day of ______________________ 20________.

____
Print name Title *(Corporate Secretary** or please print officer title)*

X ____
Signature

March 14, 2023 **PR APPROVED:**

Exhibit 10P

Form **W-9**
(Rev. October 2018)
Department of the Treasury
Internal Revenue Service

Request for Taxpayer Identification Number and Certification

▶ Go to *www.irs.gov/FormW9* for instructions and the latest information.

Give Form to the requester. Do not send to the IRS.

Print or type.
See **Specific Instructions** on page 3.

1 Name (as shown on your income tax return). Name is required on this line; do not leave this line blank.

2 Business name/disregarded entity name, if different from above

3 Check appropriate box for federal tax classification of the person whose name is entered on line 1. Check only **one** of the following seven boxes.

□ Individual/sole proprietor or single-member LLC □ C Corporation □ S Corporation □ Partnership □ Trust/estate

□ Limited liability company. Enter the tax classification (C=C corporation, S=S corporation, P=Partnership) ▶ ________

Note: Check the appropriate box in the line above for the tax classification of the single-member owner. Do not check LLC if the LLC is classified as a single-member LLC that is disregarded from the owner unless the owner of the LLC is another LLC that is **not** disregarded from the owner for U.S. federal tax purposes. Otherwise, a single-member LLC that is disregarded from the owner should check the appropriate box for the tax classification of its owner.

□ Other (see instructions) ▶

4 Exemptions (codes apply only to certain entities, not individuals; see instructions on page 3):

Exempt payee code (if any) ________

Exemption from FATCA reporting code (if any) ________

(Applies to accounts maintained outside the U.S.)

5 Address (number, street, and apt. or suite no.) See instructions.

Requester's name and address (optional)

6 City, state, and ZIP code

7 List account number(s) here (optional)

Part I Taxpayer Identification Number (TIN)

Enter your TIN in the appropriate box. The TIN provided must match the name given on line 1 to avoid backup withholding. For individuals, this is generally your social security number (SSN). However, for a resident alien, sole proprietor, or disregarded entity, see the instructions for Part I, later. For other entities, it is your employer identification number (EIN). If you do not have a number, see *How to get a TIN,* later.

Note: If the account is in more than one name, see the instructions for line 1. Also see *What Name and Number To Give the Requester* for guidelines on whose number to enter.

Social security number

□□□ – □□ – □□□□

or

Employer identification number

□□ – □□□□□□□

Part II Certification

Under penalties of perjury, I certify that:

1. The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me); and
2. I am not subject to backup withholding because: (a) I am exempt from backup withholding, or (b) I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or (c) the IRS has notified me that I am no longer subject to backup withholding; and
3. I am a U.S. citizen or other U.S. person (defined below); and
4. The FATCA code(s) entered on this form (if any) indicating that I am exempt from FATCA reporting is correct.

Certification instructions. You must cross out item 2 above if you have been notified by the IRS that you are currently subject to backup withholding because you have failed to report all interest and dividends on your tax return. For real estate transactions, item 2 does not apply. For mortgage interest paid, acquisition or abandonment of secured property, cancellation of debt, contributions to an individual retirement arrangement (IRA), and generally, payments other than interest and dividends, you are not required to sign the certification, but you must provide your correct TIN. See the instructions for Part II, later.

Sign Here **Signature of U.S. person ▶** **Date ▶**

General Instructions

Section references are to the Internal Revenue Code unless otherwise noted.

Future developments. For the latest information about developments related to Form W-9 and its instructions, such as legislation enacted after they were published, go to *www.irs.gov/FormW9.*

Purpose of Form

An individual or entity (Form W-9 requester) who is required to file an information return with the IRS must obtain your correct taxpayer identification number (TIN) which may be your social security number (SSN), individual taxpayer identification number (ITIN), adoption taxpayer identification number (ATIN), or employer identification number (EIN), to report on an information return the amount paid to you, or other amount reportable on an information return. Examples of information returns include, but are not limited to, the following.

- Form 1099-INT (interest earned or paid)
- Form 1099-DIV (dividends, including those from stocks or mutual funds)
- Form 1099-MISC (various types of income, prizes, awards, or gross proceeds)
- Form 1099-B (stock or mutual fund sales and certain other transactions by brokers)
- Form 1099-S (proceeds from real estate transactions)
- Form 1099-K (merchant card and third party network transactions)
- Form 1098 (home mortgage interest), 1098-E (student loan interest), 1098-T (tuition)
- Form 1099-C (canceled debt)
- Form 1099-A (acquisition or abandonment of secured property)

Use Form W-9 only if you are a U.S. person (including a resident alien), to provide your correct TIN.

If you do not return Form W-9 to the requester with a TIN, you might be subject to backup withholding. See What is backup withholding, *later.*

March 14, 2023

Exhibit 10P

Merchant Agreement Terms and Conditions

These terms and conditions constitute an integral part of the Merchant Processing Agreement ("Agreement"). In consideration of the covenants set forth below, Central Bank of St. Louis ("Acquirer"), which is a member of Visa U.S.A. Inc. ("Visa"), MasterCard International ("MasterCard"), Discover®, American Express® Travel Related Services Company, Inc. (AXP) or jointly with Visa/MasterCard/Discover/American Express ("Payment Card Brands") and the undersigned merchant ("Merchant") have agreed as follows as of the date of acceptance of this Agreement by TriSource Solutions, LLC d/b/a REPAY ("REPAY or ISO"), as an affiliate of Acquirer for the purposes of providing merchant services.

ARTICLE I – CARD TRANSACTIONS

1.1 Honoring Cards

A) Merchant, whether dealing with the public or otherwise, shall honor, in a non-discriminatory manner, all valid Visa/MasterCard/Discover cards, as well as cards issued in the name of American Express ("Cards") of the type(s) indicated when properly presented as payment in connection with bona fide, legitimate business transaction;

B) Merchant shall not require a Cardholder to provide identification information such as telephone number, address or driver's license number as a condition of completing a transaction unless permitted by applicable state law and allowed by the rules and regulations ("Card Issuers' Regulations") of a Card Issuer Visa/MasterCard/Discover (issuers shall hereinafter be referred to collectively as "Card Issuers");

C) Merchant may not make a photocopy of a Card under any circumstances nor request that the Cardholder provide a photocopy of the Card as a condition for honoring same.

D) Surcharging

1) Merchant must complete a Surcharge Notification form to notify the acquirer of merchant's intent to surcharge cardholder a minimum of 30 days prior to doing so. This form is located at www.repay. com

2) Merchant must complete notification to Visa at www.visa.com/merchantsurcharging

3) Merchant must complete notification to MasterCard at www.mastercard.us.merchants/support/surcharge-rules.html

4) Merchant must disclose surcharging to cardholders prominently and near the point of sale device.

5) Surcharge must be displayed on the cardholder's receipt as a separate line item while being included in the total transaction amount.

6) Merchant must NOT surcharge debit cards, prepaid cards or check cards.

7) Merchant MAY NOT surcharge cardholder an amount which is more than the merchant is charged. Also a maximum cap of 4% applies.

8) Merchant agrees to refund surcharge amount on a transaction which is refunded. Merchant agrees to partially refund a surcharged amount pro rata on a partially refunded transaction.

9) Merchant agrees if a transaction with a surcharge amount is disputed, the total transaction will be charged back including the surcharged amount.

10) Merchant agrees not to surcharge cardholders if specifically prohibited by state law in which the business is governed.

11) Merchant agrees these rules not are totally inclusive, and Merchant agrees to read and understand the to-tality of each payment card brand's rules by visiting each website PRIOR to engaging in surcharging any cardholders.

E) The Card Brands permit any U.S. merchant to set a minimum transaction amount (not to exceed USD 10 or any higher amount established by the Federal Reserve by regulation) to accept cards that access a credit account. The Brands do not permit merchants to set a minimum transaction amount to accept cards that access a debit account.

1.2 Advertising

A) Subject to: i) private clubs, ii) Merchants who do not deal with the public, iii) vehicle leasing companies at airport locations, iv) transportation companies subject to government regulation, or v) Merchants expressly exempted from by Card Issuers' Regulations, Merchant shall adequately display advertising or promotional material provided or required to inform the public that Cards are honored at Merchant's place of business;

B) Merchant shall not display or use advertising or promotional materials containing Acquirer's name or symbol, which might cause a customer to assume that Merchant honors only Cards issued by Acquirer;

C) Merchant shall have the right to use or display the proprietary names and symbols associated with Cards only while this Agreement is in effect, or until Merchant is notified by Acquirer or any appropriate Bank Card organization to cease such usage;

D) Merchant shall comply with all applicable Card Issuer Regulations concerning the use of service marks and copyrights owned by Visa/MasterCard/Discover;

E) Merchant shall use the proprietary names and symbols associated with Cards only to indicate that Cards are accepted for payment and shall not indicate, directly or indirectly, that Acquirer, Visa/MasterCard/Discover or any Payment Card organization endorses Merchant's products or services;

F) Merchant shall not refer to Visa/MasterCard/Discover in stating eligibility for its products, services, or memberships.

1.3 Card Examination

A) Merchant agrees to carefully examine any Card security features (such as hologram) included on the Card; compare the embossed account number on the face of the Card with the account number indented on the signature panel; check the validity date and expiration date of the Card; and shall not honor any invalid or expired Card without proper, prior authorization;

B) Where the magnetic stripe on the Card is read in connection with a transaction, Merchant shall compare the embossed account number on the Card to the number displayed or printed by the terminal to verify they are the same;

C) Except for mail orders, telephone orders or pre-authorized transactions, Merchant shall not complete a transaction without presentation of the Card by the Cardholder and proper examination by the Merchant of the Card;

D) If the signature panel on the Card is blank, Merchant shall:

1) Review the positive identification to confirm identity. Such identification must consist of a current, official government identification document (such as a passport or driver's license) bearing Cardholder's signature; and

2) Indicate such positive identification (including any serial numbers and expiration date) on the sales draft if the transaction is a Visa transaction, and if permitted by applicable state law. (Such information shall not be recorded for MasterCard transactions); and

3) Require Cardholder to sign the signature panel on the Card before completing the transaction; and

4) Request authorization.

E) In the case of a Visa Card, Merchant shall compare the printed issuing bank identification number, which is directly above the first four digits of the embossed account number. If the printed number and the embossed number do not match, Merchant shall call the voice authorization number and request a "code 10" operator.

1.4 Authorization

A) Before honoring any Card, Merchant is required to request authorization from Acquirer's designated authorization center.

B) Authorization numbers, or positive account number verification response codes, as appropriate, shall be printed legibly in the designated area on the sales slip.

C) If authorization is denied, Merchant shall not complete the transaction and shall use its best efforts by reasonable and peaceful means to follow any instructions from the authorization center.

D) Merchant shall be liable to Acquirer, regardless of any authorization, if Merchant completes a transaction when the Cardholder is present but does not have his Card, the Cardholder does not sign the sales slip, or the signature on the sales slip does not match the signature appearing on the Card, or the signature panel on the Card is blank.

E) In no event shall an authorization be deemed to be Acquirer's representation that the particular transaction is in fact a valid, authorized or undisputed transaction entered into by the Cardholder or an authorized user of the Card.

F) Where authorization is requested for transaction involving suspicious or unusual circumstances the Merchant shall call and request a "code 10" authorization from Acquirer's designated authorization center.

G) An authorization for a restaurant transaction, in which a gratuity is added to the sales slip by the Cardholder, is valid if the total transaction amount is within 20% of the authorization amount.

H) If authorization is obtained for the estimated amount of a car rental transaction, Merchant shall disclose to Cardholder the amount authorized on the rental date.

1.5 Retention and Retrieval of Cards

Merchant shall use its best efforts, by reasonable and peaceful means, to retain or recover a Card;

A) If Merchant receives a negative response from the account number verification service, and until Merchant receives further instruction from Acquirer's designated authorization center;

B) While making an authorization request;

1) If Merchant is advised to retain the Card in response to an authorization request; or

2) Where the embossed account number, indent printed account number and/or encoded account number do not match, or an unexpired Card does not have the appropriate hologram on the Card face; or

3) If the Merchant has reasonable grounds to believe the Card is counterfeit, fraudulent or stolen. The obligation of Merchant to retain or recover a Card imposed by this section does not authorize a breach of the peace or any injury to persons or property, and Merchant will hold Acquirer harmless from any claim arising from any injury to person or property or other breach of the peace. If a recovered Card is retained by a law enforcement agency, Merchant shall forward a legible copy of the front and back of the Card to Acquirer, or other bankcard organization, as appropriate, to support payment of any applicable reward.

1.6 Completing the Transaction Record

Except as provided below, Merchant agrees to do all of the following when honoring a Card; provided, however, that Merchant shall have no obligations to utilize a sales Slip (and the provisions below relating to usage of sales slips shall not apply to Merchant) if Merchant does not utilize sales slip documents in its nonnal course of business;

A) To enter on the sales slip the transaction date, a description of the goods or services sold, and the price thereof (including any applicable taxes) in detail sufficient to identify the transaction;

B) To obtain the signature of the customer on the sales slip after the transaction amount is identified in the "total" column;

C) To compare the signature on the sales slip and the signature panel of the Card, and if the Card has a photograph of the Cardholder, to verify identity, and if either identification is uncertain or the account numbers are not the same or Merchant otherwise questions the validity of the Card, to contact Acquirer's authorization center for instructions;

D) To imprint legibly on the sales slip the embossed legends from the Card and from the Merchant imprinter plate. If the imprinter does not legibly imprint, Merchant shall legibly detail the Cardholder's name and account number and Merchant's name and place of business, as well as the name or trade style of the issuer as it appears on the face of the Card, the ICA number, the Card initials, if any, and both the effective date and expiration date. Merchant shall also record on the sales slip any other embossed data such as security symbols.

E) To deliver a true and completed copy of the sales slip to the customer at the time or delivery of the goods or performance of the services or for point of transaction terminal transactions, at the time of the transaction.

F) For transactions, which originate at and are data-captured using point-of-sale transaction terminals. Merchant must include the following on the Cardholder copy or the sales draft;

1) The Cardholder account number

2) Merchant's name

3) Merchant's location code or city and state

4) The amount of the transaction

5) The transaction date

G) Transaction records must be produced for all transactions, which originate at and are data-captured using automated dispensing machines or limited-amount terminals, except for transactions that originate at magnetic-stripe-reading telephones. Such transaction records must include at least the following information;

1) The Cardholder account number

2) Merchant's name

3) The magnetic-stripe-reading terminal location code or city and state

4) The amount of the transaction

5) The transaction date

H) Whenever the encoded account number cannot be read from the magnetic stripe, Merchant shall follow normal authorization procedures and complete the approved transaction using a manual imprinter.

1.7 Multiple Transaction Records; Partial Consideration

A) Merchant must include on one transaction record the entire amount due for the transaction, except in the following instances:

1) The transaction involves purchases made in separate departments of a multi-department store;

PR APPROVED:

March 14, 2023

Exhibit 10P

2) The transaction involves delayed or amended charges for a vehicle rental transaction in which:
   a) The Cardholder consented to be liable for such charges; and
   b) Such charges consist of ancillary or corrected charges such as taxed or fuel fees, and not charges for loss, theft, damage, or traffic violations;
3) Merchant sends the Cardholder a copy of the amended or add-on sales drafts (sales drafts for such delayed or amended charges may be deposited without the Cardholder signature provided that Merchant has Cardholder's signature on file, and the words "SIGNATURE ON FILE" are entered onto the signature panel of the sales draft);
4) The customer pays a portion of the transaction amount in cash, by check, with any Card, or any combination of such payments at the time of the transaction and further provided that Merchant obtains authorization for that part of the transaction effected with a Card;
5) All or a portion of the goods or services are to be delivered or performed at a later date and the customer signs two separate sales slips, one of which represents a deposit and the second of which represents payment of the balance, and the balance sales slip is completed only upon delivery of the goods or performance of the services, in which case Merchant agrees:
   a) To note on the sales slips the word "Deposit" or "Balance" as appropriate and the words "Delayed Delivery"
   b) If the total amount or the two slips exceeds the applicable floor limit, to obtain prior authorization and note the authorization date an approval code in the sales slips; and
   c) Not to present the "Balance" sales slip until all goods are delivered or all the services are performed; or
   d) The Cardholder is using the installment payment option offered in accordance with Paragraph 1.8.
   e) Merchant agrees not to divide a single transaction between two or more transaction records to avoid obtaining an authorization.
   f) For sales processed at electronic POS terminals, multiple items individually billed to the same account will not be considered a violation of this Agreement if separate authorizations are obtained for each item.

1.8 Telephone Order, Mail Orders, Preauthorized Orders, and Installment Orders

A) If the transaction is a telephone order (TO) mail order (MO), or preauthorized order (PO), the sales slip may be completed without a customer's signature or a Card imprint, however Merchant shall:
   1) Print legibly on the sales slip sufficient information to identify the Card issuer, Merchant and the Cardholder, including: Merchant's name and address, the Card issuers' name or trade style, ICA number and bank initials (if any), the account number, the expiration date and any effective date on the Card, the Cardholder's name, and any company name, and
   2) Print legibly on the signature line of the sales slip the letter "TO","MO" or "PO" (recurring transaction for Visa transaction), as appropriate.
   3) Obtain authorization for every sale for MO and TO transactions, authorization must be obtained no more than 7 calendar days before the transaction date. Merchant shall attempt to obtain the expiration date of the Card as part of the authorization inquiry.

B) On any non imprinted or expired Card transaction, Merchant shall be deemed to warrant the customer's true identity as an authorized user of the Card, whether or not authorization is obtained, unless Merchant obtains and notes legibly on the sales slip independent evidence of the customer's true identity.

C) In connection with a recurring transaction (or pre-authorized order) pursuant to which goods or services are delivered to or performed for a Cardholder periodically, Merchant agrees to the following conditions:
   1) Merchant must obtain a written request from the Cardholder that the recurring transaction is charged to the Cardholder's account;
   2) The written request must specify the amount of the recurring transaction (or allow space for Cardholder to specify a minimum and maximum amount if the recurring transactions are to be for varying amounts), the frequency of the recurring charges, and the length of time for which the preauthorized order is to remain in effect;
   3) Before renewing a preauthorized order, Merchant must obtain a subsequent written request from the Cardholder containing the information listed above;
   4) Merchant must not deliver goods or perform services covered by a preauthorization order after being advised that the preauthorization has been canceled by cardholder or that the Card is not being honored; and
   5) Except as provided in Paragraph 1.7, a recurring transaction may not include partial payments to Merchant for goods or services purchased in a single transaction, or for periodic payments of goods or services on which Merchant assesses additional finance charges;
   6) Merchant must inform Cardholder that he has the right to receive, at least 10 days prior to each scheduled transaction date, written notice of the amount and date of the next charge. Cardholder may elect to receive the notice
      a) For every charge
      b) Only when the transaction amount does not fall within the specified range shown on the order form, or If the total
      c) Only when the transaction amount will differ from the most recent charges charge by more than an agreed upon amount.

D) Merchant may offer Cardholders an installment payment option for its mail/telephone order merchandise subject to the following conditions; Merchant's promotional material must clearly disclose the installment terms, including but not limited to:
   1) Whether the plan is available only for selected items or for the total amount or any order; and
   2) How shipping and handling charges and applicable taxes will be billed. The material also must advise Cardholders who are not billed in the transaction currency of the Merchant that the installment billing amounts may vary due to fluctuations in the currency conversion rates;
   3) Merchant may add no finance charges. The sum of the installment transactions may not exceed the total sales price of the merchandise on single transaction bases;
   4) Authorization is required for each installment transaction. Merchant's floor limit is zero;
   5) Merchant may not deposit the first installment transaction with Acquirer until the merchandise is shipped. Subsequent installment transactions must be deposited;
   6) At intervals of 30 days or more; or
   7) On the anniversary date of the transaction {i.e. the same date each month}
   8) In addition to Merchant's name, an appropriate installment transaction descriptor (e.g. 1 of 5, 2 of 5) must be included in the Merchant mane field of the clearing record.

1.9 Vehicle Rental Transactions

Regardless of the terms and conditions of any written preauthorization form, the sales slip amount for any vehicle rental transaction shall include only that portion or the transaction, including any applicable taxes, evidencing a bona fide renting of personal property by Merchant to a customer and shall not include any consequential charges. Nothing herein is intended to restrict Merchant from enforcing the terms and conditions of its preauthorization form through means other than a Card transaction.

1.10 Returns and Adjustments; Credit Slips

A) If with respect to any transaction, any merchandise is accepted for return or any services are terminated or canceled, or any price adjustment is allowed by the Merchant (other than involuntary refunds by airlines or other carriers when required by applicable tariffs and except where otherwise required by law or governmental regulations.) Merchant shall not make any cash refund to the Cardholder but shall deliver promptly to Acquirer a credit slip evidencing such a refund or adjustment.

B) Each credit slip shall be signed and dated by Merchant and include the transaction date, a description of the goods returned, services canceled or adjustment made and the amount or the credit in sufficient detail to identify the transaction and the embossed data from the Card and Merchant's imprinter plate

C) The refund or adjustment shall be indicated on a credit slip and may not exceed the original transaction amount.

D) The Merchant may limit its return, adjustment, refund or exchange policies provided that proper disclosure is made and purchased goods or services are delivered to the Cardholder at the time of the transaction.

E) Proper disclosure by the Merchant must be given at the time of the transaction by printing the following words or similar wording on all copies of the sales slip or invoice being presented to the Cardholder for signature in letters approximately 1/4 inch high and in close proximity to the space provided for the Cardholder's signature;
   1) "NO REFUND" for a Merchant which may not accept merchandise in return or exchange and may not issue a refund to a Cardholder.
   2) "EXCHANGE ONLY" for a Merchant which may accept merchandise in immediate exchange for similar merchandise of a price equal to the amount of the original transaction
   3) "IN STORE CREDIT ONLY" for a Merchant which may accept merchandise in return and deliver to the Cardholder an In-store credit for the value of the merchandise returned which may be used only in the Merchant's place(s) of business

F) A Merchant may, if permitted by applicable law, stipulate special circumstances under which a surcharge shall be assessed for the use of a Card. The wording to appear on the sales slip shall be any special terms of the transaction(s).

G) Merchant must deliver to the Cardholder a true and completed copy of the credit slip to the time of the credit transaction. Merchant shall not process a credit slip without having completed the purchase transaction with the Cardholder and in no event may the credit exceed the amount of the original transaction.

1.11 Cash Payments

Merchant shall not receive any payments from a customer for charges included on any transaction record resulting from the use of any Card, nor receive any payments from a Cardholder to prepare and present a credit slip for the purpose or affecting a deposit to the Cardholder's account.

1.12 Cash Advances

Unless expressly authorized in writing by Acquirer, Merchant agrees not to make any cash advance to a Cardholder, either directly or by deposit to the Cardholder's account. Money orders sent by wire, contribution to charitable and political organizations, tax payments, insurance premium payments, alimony and child support payments, and court costs and fines shall not be considered cash advances or withdrawals. Merchant shall not obtain, under any circumstance, authorization for nor process a sale or cash advance on any card Merchant is authorized to use. Processing Merchant's own card or the processing of an unauthorized cash advance is grounds for immediate termination.

1.13 Disclosure and Storage of Transaction Information

A) Except as otherwise required by law, Merchant shall not, without the Cardholder's and Acquirer's prior written consent, sell, purchase, provide, or otherwise disclose the Cardholder's account information or other Cardholder information to any third party other than Acquirer's or Merchant's agents and processing organizations for the purpose of assisting Merchant in its business.

B) Merchant and any agent of Merchant shall store in an area limited to selected personnel and prior to discarding, shall destroy in a manner rendering data unreadable all material containing Cardholder account number Card imprints, such as sales slips and credit slips, car rental agreements and carbons.

C) Merchant or any agent of Merchant shall not retain or store magnetic stripe data subsequent to the authorization of a transaction.

D) Merchant further warrants and agrees that in the event of its failure, including bankruptcy, insolvency or other suspension of business operations, it will not sell, transfer, or disclose any materials that contain Cardholder account numbers, personal information or transaction information to any third parties, and shall return the information to Acquirer or provide acceptable proof of destruction to Acquirer.

E) Merchant shall notify Acquirer if it utilizes any third party or third party software products to process, store or transmit any information with respect to transactions.

F) Acquirer shall not disclose or permit access to or use of the non-public personal information of Merchant or its members or customers made available by Merchant to Acquirer for any purposes other than those specifically required to fulfill acquirer's contractual obligations with Merchant. Acquirer shall not sell the information regarding Merchant or its members or customers for any reason. In connection with providing services to Merchant, Acquirer shall comply with Section 3.10 and take all commercially reasonable steps to ensure the privacy and security of the information of Merchant and its members or customers In Acquirer's possession and protect against anticipated threats and hazards to the security of such Information. Acquirer shall take all commercially reasonable steps to prevent unauthorized access to or use of such information that could result in substantial harm or inconvenience to Merchant or its members or customers. In the event any court or regulatory agency seeks to compel disclosure of the Information, Acquirer shall, if legally permissible, promptly notify Merchant of the disclosure requirement and will cooperate so that Merchant may at its expense seek to legally prevent this disclosure of the information.

ARTICLE II – PRESENTMENT PAYMENT AND CHARGEBACK

2.1 Transmission of Data

In lieu of depositing paper sales slips and credit slips with Acquirer, Merchant may transmit to Acquirer, in the form of magnetic tape or electronic data, as specified and acceptable to Acquirer, all data required to appear on the sales slip or credit slip. The term "sales data" as used herein shall mean the data transmitted by Merchant contained in a sales slip or the electronic or magnetic tape record that is the equivalent of such sales slip. The term "credit data" as used in this Agreement shall mean the data transmitted by Merchant contained in a credit slip or the electronic or magnetic tape record that is equivalent thereto. All data (transaction records) transmitted shall be pre-sorted and

PR APPROVED:

March 14, 2023

Exhibit 10P

organized in a form and format approved and/or instructed in advance by Acquirer. All references to "sales slips" and "credit slips" in this Agreement shall be deemed to include transaction records transmitted by paper, electronically or on magnetic tape.

2.2 Presentment of Transaction Records to Acquirer

A) Merchant may designate a third party who does not have a direct Agreement with Acquirer as its agent for delivering transactions data-captured at the point of sale by such agent if Merchant elects to use such agent. Merchant agrees to the following conditions (for purposes of this Paragraph 2.2, "Merchant" includes any such permitted agent):
  1) Merchant must provide satisfactory notice to Acquirer that Merchant chooses to exercise the option specified above;
  2) The obligation of Acquirer to reimburse Merchant for transactions is limited to the amount (less the applicable or appropriate discount fee) delivered by Merchant's designated Agent; and
  3) Merchant is responsible for its agent's failure to comply with applicable Credit Card Issuer and/or Merchants Regulations, including, but not limited to, any violation resulting in a chargeback.

B) Merchant shall present all sales data relevant to a transaction, except that;
  1) Merchant shall present no sales data until goods have been shipped or the services have been performed and Merchant has otherwise performed all of its principal obligations to the customer in connection with the transaction unless the Cardholder agreed to a delayed delivery of goods and proper disclosures were made at the time of the transaction;
  2) When Merchant requests and receives authorization for delayed presentment and legibly prints on the sales slip the authorization number and the words "Delayed Presentment", Merchant must present the sales data within the permitted period for delayed presentment (not to exceed 30 calendar days).
  3) If Merchant is obligated by law to retain a sales slip or return it to a buyer upon timely cancellation, Merchant must present the sales data within 10 bank business days after the date of the transaction; and
  4) When Merchant has multiple locations or offices and accumulates transaction records at a central facility, Merchant must present the transaction records to Acquirer within 20 calendar days after the transaction date. Merchant with multiple locations must deliver the transaction records in such manner that Acquirer is able to identify the transactions originating at each location.

C) Merchant shall deliver all credit data to Acquirer within 3 bank business days after the credit transaction date, except if Merchant has multiple locations as described in Paragraph (B / 4) above, Merchant must deliver the credit data to Acquirer within 7 business days after the transaction date

D) Merchant shall not present to Acquirer, directly or indirectly, any transaction record that Merchant knows or should have known: to be fraudulent or not authorized by the Cardholder; results from transaction outside Merchant's normal course of business; that results from a transaction not involving Merchant; that contains the account number of a Card account issued to Merchant; or was not the result of a transaction between Merchant and Cardholder.

E) If the transmission of sales data or credit data from Merchant to Acquirer is in the form of magnetic tape or electronic data, Merchant shall preserve a copy of the sales and credit slips pursuant to Paragraph 3.3.

F) Merchant is prohibited from re-depositing any transaction that has previously been charged back and subsequently returned to Merchant. This prohibition applies with or without the Cardholder's consent of the Merchant's actions. Merchant may, at its option, pursue payment from the customer in such event.

G) Merchant shall not deposit duplicate Transactions. Merchant shall be debited for any duplicate Transactions and shall be liable for any Chargebacks and any fines or penalties levied by the Payment Card Brands, which may result therefrom.

H) Merchant shall not present any Transaction representing the refinancing of an existing obligation of a Cardholder including, but not limited to obligations:
  1) Previously owed to Merchant,
  2) Arising from the dishonor of a Cardholder's personal check, and/or
  3) Representing the collection of any other pre-existing indebtedness, including collection of delinquent accounts on behalf of third parties.

2.3 Acceptance and Discount

Subject to the provisions of any agreement of Merchant hereunder and of any chargeback right, Acquirer agrees to accept valid transaction records from Merchant during the term of this Agreement and to pay Merchant the total amount represented by the transaction records less any percentage discount and fees agreed to by the parties. In this regard, Merchant understands and agrees that any fee or charge provide herein is that which is to be initially applicable and imposed and such fees and charges may be increased or otherwise amended from time to time by Acquirer with or without advance notice to Merchant except as otherwise herein specifically provided. Any payment made by Acquirer to Merchant shall not be final but shall be subject to subsequent review and verification by Acquirer and may be subject to chargeback until the chargeback period expires.

2.4 Insecurity

Notwithstanding Paragraph 2.3, Acquirer may withhold payment to Merchant or prohibit Merchant's withdrawal of funds then on deposit with Acquirer for any of the following reasons:

A) Acquirer is suspicious of any transaction records;

B) Merchant's volume of sales exceeds a stipulated amount or amounts that are typically generated during a particular period;

C) Merchant's average ticket amount exceeds a stipulated amount;

D) Merchant does not swipe Cards through electronic terminals;

E) Merchant fails to authorize transaction;

F) Acquirer receives excessive retrieval request against Merchant's account as prior activity;

G) Excessive chargebacks are debited against Merchant's account as prior activity; or

H) If for any other reason, including but not limited to fines or penalties that are, or Acquirer reasonably assumes will be, assessed against Merchant based on its violation of any Card Issuer Regulations, and/or its breach of this Agreement such that Acquirer reasonably determines that withholding funds or preventing withdrawals of funds previously deposited with Acquirer is necessary to cover anticipated charges, fines and/or penalties resulting from Merchant's Card activities.

2.5 Endorsement

Merchant agrees that Merchant shall be deemed to have endorsed in Acquirer's favor any transaction records Merchant presents to Acquirer and Merchant hereby authorizes Acquirer to supply such endorsement on Merchant's behalf.

PR APPROVED:

2.6 Prohibited Payment

Merchant agrees that Acquirer has the sole right to receive payments on any accepted transaction record as long as:

A) Acquirer has paid Merchant the amount represented by the transaction record less the discount and fees; and

B) Acquirer has not charged such transaction record back to Merchant unless specifically authorized in writing by Acquirer. Merchant agrees not to make or attempt to make any collections on any transaction record, and promptly to deliver the same in kind to Acquirer as soon as received, together with the Cardholder's name and account number and any correspondence accompanying the payment.

C) A merchant may not accept a Card for an unlawful Internet gambling transaction.

D) Merchant will pay all Card Association fines, fees, penalties and all other assessments or indebtedness levied by Card Associations to Bank which are attributable, at the Bank's discretion, to Merchant's Transaction processing or business.

2.7 Chargeback

A) Under any one or more of the following circumstances, Acquirer has accepted, and Merchant shall repay Acquirer the amount represented by the transaction record:
  1) The transaction record or any material information on a sales slip (such as the account number, expiration date of the Card, Merchant description, transaction amount, or date), is illegible, incomplete, is not endorsed, or is not delivered to Acquirer within the required time limits;
  2) The transaction received a negative account verification service response (or would have received a negative account verification service response if Merchant had contacted the service on the transaction date) and Merchant did not reject the transaction or receive prior authorization for the transaction, as applicable;
  3) The sales slip does not contain the required imprint of a Card that was valid, effective, and unexpired on the transaction date;
  4) The transaction was one for which prior credit authorization was required and prior credit authorization was not obtained, or a valid authorization number is not correctly and legibly included on the transaction record;
  5) The transaction record is a duplicate of an item previously paid, or is one of two or more transaction records generated in a single transaction in violation of this Agreement;
  6) The Cardholder disputes the execution of the transaction record, the sale, delivery, quality, or performance of the goods or services purchased, or alleges that a credit adjustment was requested and reissued or that a credit adjustment was issued by Merchant but not posted to the Cardholder's account;
  7) The price of the goods or services shown on the transaction record differs from the amount shown on the copy of the sales slip or the receipt delivered to the customer at the time of the transaction;
  8) Acquirer reasonably determines Merchant has violated any term, condition, covenant, warranty, or other provision of this Agreement in connection with the transaction record or the related transaction;
  9) Acquirer reasonably determines the transaction record is fraudulent or that the related transactions were not a bona fide transaction in Merchant's ordinary course of business, or is subject to any claim of illegality, cancellation, recession, avoidance, or offset for any reason whatsoever, including without limitation negligence, fraud, or dishonesty on the part of Merchant or Merchant's Agents or employees;
  10) The transaction record arises from a mail or telephone order transaction which the Cardholder disputes entering into or authorizing, or which involves an account number that never existed or that has expired and has not been renewed;
  11) Merchant fails to provide any sales slip or credit slip to Acquirer in accordance with Paragraph 3.1 of this Agreement.
  12) Any other Merchant transaction charged back to Acquirer for whatever reason pursuant to Card Issuer Regulations.

B) In the event Merchant believes a chargeback to be improper, Merchant must notify Acquire of this in writing within 10 calendar days of the date of the chargeback or forfeit its right to contest the chargeback.

C) Except in the case of chargebacks based solely on the Merchant's failure to obtain an authorization, Acquirer may chargeback a transaction in accordance with this section even if an authorization was obtained in connection therewith. Merchant's obligation to reimburse, indemnify Acquirer for the amount of any chargeback shall survive termination of this Agreement.

D) Guarantors are personally liable for all chargebacks. In the event Merchant sells its business, and the new owner incurs chargebacks from transactions during the period Guarantors owned business, the original Merchant and all guarantors will continue to be held personally liable for the chargebacks.

2.8 Merchant's Business

A) Merchant shall provide Acquirer and REPAY with immediate notice of its intent to
  1) Transfer or sell any substantial part of its total assets, or liquidate;
  2) Change the basic nature of its business, including selling any products or services not related to its current business;
  3) Change fifty percent (50%) or more of the ownership or transfer control of its business;
  4) Enter into any joint venture, partnership or similar business arrangement whereby any person or entity not a party to this Agreement assumes any interest in Merchant's business; or
  5) Alter in any way Merchant's approved monthly volume and average ticket;

B) Failure to provide notice as required above may be deemed a material breach and shall be sufficient grounds for termination of this Agreement, or, at REPAY option may result in REPAY amending the terms of this Agreement, including, but not limited to, holding funds and/or altering the Merchant funding schedule if REPAY and Acquirer deem it necessary to protect against financial loss. If any of the changes listed above occur, Acquirer and REPAY shall have the option to re-negotiate the terms of this Agreement or provide immediate notice of termination;

C) Failure to provide REPAY with the merchant's correct federal tax identification number(s) with the completed processing application may result in fines assessed to the merchant. Moreover, failure to provide REPAY with an updated federal tax number(s) for the merchant within 15 days of any change may result in fines assessed to the merchant;

D) Merchant will immediately notify REPAY, with a copy to Acquirer, of any bankruptcy, receivership, insolvency or similar action initiated by or against Merchant or any of its principals. Merchant will include Acquirer and REPAY on the list of creditors filed with the Bankruptcy Court, whether or not a claim exists at the time of filing;

E) Merchant must notify REPAY, with a copy to Acquirer, in writing of any changes to the information in the Merchant Application, including but not limited to: any additional location or new business, the identity of principals and/or owners, the form of business organization, type of goods and services provided, and how sales are completed. Merchant must also notify REPAY in writing, with a copy to Acquirer, if Merchant sells or closes its business. Except for a change to the financial condition, REPAY and Acquirer must receive all such notices 7 days before the change. Merchant will provide updated information

Exhibit 10P

to REPAY upon request. Merchant is liable to REPAY and Acquirer for all losses and expenses incurred by REPAY and Acquirer arising out of Merchant's failure to report changes. REPAY and Acquirer may immediately terminate this Agreement upon a change to the information in the Merchant Application, whether REPAY and Acquirer independently discover such change or whether Merchant notifies REPAY and Acquirer of such change.

ARTICLE III – MISCELLANEOUS

3.1 Imprinters and Terminals

A) Merchant shall keep all imprinter(s) and terminal(s) used to process Card transactions in good working order and shall notify Acquirer prior to any change in imprinted or programmed information.

B) Merchant is required to immediately notify in writing Acquirer in the event a Point of Sale terminal becomes lost or stolen.

3.2 Forms

Merchant shall use only such forms or modes of transmission for sales data and credit data as are provided or approved in advance by Acquirer, and Merchant shall not use forms or equipment provided by Acquirer other than in connection with Card transactions hereunder.

3.3 Records

A) Merchant shall, for Visa/MasterCard/Discover purposes, preserve a copy of the actual paper sales slips and credit slips for at least 6 months after the date Merchant presents the transaction data to Acquirer, and Merchant shall make and retain for at least 3 years from such date legible microfilm copies of both sides of such actual paper transaction records.

B) Merchant agrees to immediately notify Acquirer of any Merchant location(s) added after the date of this Agreement, and agrees to the establishment of a separate processing account for said location(s).

3.4 Request for Copies

A) Within 1 business day of receipt of any request by Acquirer, Merchant shall fax or mail to Acquirer either the actual paper transaction record, if requested by Acquirer, or a legible copy thereof (in size comparable to the actual paper transaction records), and any other documentary evidence available to Merchant and reasonably requested by Acquirer to meet its obligations under law (including its obligations under the fair credit billing act) or otherwise to respond to questions concerning Cardholders accounts.

B) For purposes of retrieval or records, Merchant must retain sale slips and credit slips by reference number within date sequence.

C) If Merchant does not provide a requested copy of sales slip(s) to Acquirer within the time frame specified, in addition to other rights and remedies available to Acquirer under this Agreement:
   1) Acquirer may charge Merchant a penalty fee; and
   2) Acquirer may charge Merchant the transaction amount of the requested sales slip.
   3) Acquirer may, at its option, charge Merchant the transaction amount of the requested sales slip at the time of the request. Such amount will be reimbursed to the Merchant upon delivery of a valid and correct sales slip.

3.5 Disputes with Cardholder; Indemnification of Acquirer

All disputes between Merchant and any Cardholder relating to any Card transaelion shall be settled between Merchant and such Cardholder. Merchant shall defend, indemnify and hold Acquirer harmless from all claims, liabilities, damages, losses (including but not limited to those arising from fraud or similar activities whether or not Merchant participated in any way), and expenditures (including but not limited to investigation expenses, resaarch time, reasonable attomey's fees and other costs of defense whether or not provided by Acquirer's personnel or others) relating to or arising out of any such Card transactions and/or from Merchant's failure to comply with any of its obligations under this Agreement. The obligations under this Paragraph 3.5 shall survive termination of this Agreement.

3.6 Excessive Chargebacks and/or Retrievals

Merchant agrees that in the event Acquirer is presented, during any monthly period, with chargebacks and/or retrieval requests relating to the transactions of the Merchant processed by Acquirer in excess of one percent (1%) of interchange volume of such transactions, such chargeback and/or retrieval requests will conclusively be deemed to be excessive under applicable Card Issuer Regulations which shall allow Acquirer to take such action as may be authorized herein or by applicable Card Issuer Regulations, including, but not limited to, terminating this Agreement and/or passing through to Merchant any charges and/or penalties that may be imposed by Visa/MasterCard/Discover. In addition to any other remedies provided herein, Acquirer may impose an excessive chargeback fee of Twenty-Five Dollars ($25) per occurrence if Merchant's monthly chargeback volume exceeds one percent (1%) of monthly sales.

3.7 Terms, Termination and MATCH and/or the Consortium Merchant Negative File (the CMNF) published by Discover (formerly Combined Terminated Merchant Files "CTMF")

A) The initial term of this Agreement shall be two (2) years from the date this Agreement is executed by Acquirer. Thereafter, the Agreement will automatically renew on a month to month basis until either party provides thirty (30) days' prior notice to the other party of its intention to terminate. Merchant's obligations under this Agreement remain in full force and effect relative to all transactions submitted under this Agreement prior to the date of termination. This Agreement may be terminated at any time by either party with or without cause upon ninety (90) days' written notice to the other party. Such notice shall be effective when hand delivered or three (3) days following the date the notice is deposited in the mail or upon any late date specified in the notice. Acquirer may terminate this Agreement without prior notice in the event Merchant is or becomes bankrupt or is unable to pay its debts as they become due, or if Acquirer reasonably determines that Merchant has violated any term, condition, covenant, or warranty of this Agreement and fails to cure such breach within thirty (30) days' notice.

B) Upon the effective date of any such termination, Merchant's rights hereunder to make Card transactions, to deposit transaction records with Acquirer, and to use sales slip forms, credit slip forms, promotional material, and any other items provided by Acquirer hereunder shall cease, but Merchant's obligations in connection with any transaction record accepted by Acquirer (whether before or after such termination), including without limitation Merchants chargeback obligations, shall survive such termination.

C) Merchant expressly acknowledges that a MATCH/CMNF file is maintained by Visa/MasterCard/Discover containing information on Merchants terminated for one of more reasons specified in Visa/MasterCard/Discover operating rules and regulations. Such reasons generally include, but are not limited to; fraud, counterfeit paper, unauthorized transaction, excessive chargebacks or highly suspect activity. Merchant acknowledges that Acquirer is required to report the Merchant business name and the names of its principals to MATCH/CMNF when Merchant is terminated due to one or more of the foregoing reasons. Merchant expressly agrees and consents to such reporting by Acquirer in the event of the termination of this Agreement due to one or more of such reasons.

3.8 Limitation of Liability

Acquirer's liability to Merchant or to any party claiming by, through or under Merchant, shall be limited in the aggregate for the term of this Agreement (as may be extended) to the average of one month's fees paid by the Merchant for the services rendered hereunder by Acquirer. In determining the average of the month's fees, the fees paid for the three months' ending on the last day of the month immediately preceding the month in which Acquirer first sends notice of a claim to Merchant shall be averaged. This Agreement is a service agreement. Acquirer disclaims all other representations or warranties made to Merchant or to any other person. **Acquirer shall in no event be liable for any incidental, exemplary, punitive, indirect or consequential damages whatsoever, regardless of whether such damages were foreseeable or whether any party or entity has been advised of the possibility of such damages.** Acquirer is not liable to Merchant for errors made by account number verification service or for Merchants failure to contact same. The above limitations shall not apply to a breach by Acquirer of Sections 1.13(F) or 3.10 or to an indemnification obligation of Acquirer.

3.9 Supplementary Documentation; Fees; Fines and Penalties

All reference herein to this "Agreement" shall collectively include current schedules, amendments, Merchant application, change notices, addendum, appendices and attachments and associated reference materials, all or which are incorporated herein by reference and made a part of this Agreement as if fully set forth. Merchant agrees to pay the fees and charges identified in this Merchant application or in any other schedule of fees and charges provided to Merchant, which may be amended from time to time as provided in Paragraph 3.18. All fees and charges charged to the Merchant shall be presumed correct unless the Merchant notifies Acquirer in writing within thirty (30) days from the date of a monthly statement which includes the disputed item. Merchant shall be liable to Acquirer for all fees, fines and penalties that may be assessed against Acquirer by either Visa/MasterCard/Discover as a result of Merchant's activities hereunder. An administrative fee will be applicable.

3.10 Compliance with Law; PCI Security Program, Non-Disclosure and Storage of Cardholder and Transaction Information Requirements

Each party confirms that it is, and shall be, in full compliance during the term of this Agreement with all laws, statutes and federal and/or state regulations, as well as rules and operating regulations and bylaws imposed by Visa/ MasterCard/Discover applicable to its business and any Card transaction, including without limitation all state and federal consumer credit and consumer protection statutes and regulations, non-disclosure of Cardholder information and transaction documents, and other security procedures adopted by Visa/MasterCard/Discover. Merchant hereby certifies that it (and any outside agent that it may utilize to submit transactions to Acquirer and/or third party software provider) complies with the Payment Card Industry ("PC I") instituted by Visa/MasterCard/ Discover hereby certifies that it (and any outside agent that it may utilize to process transactions submitted to Acquirer and/or third party software provider) complies with the Payment Card Industry ("PCI") instituted by Visa/MasterCard/Discover, including the PCI Cloud Computing Standards. Each Party hereby agrees to pay any fines and penalties that may be assessed by Visa/MasterCard/Discover as a result of such party's breach of this paragraph, including but not limited to any fines or penalties that may be assessed based on its noncompliance with the requirements of PCI, or by its failure to accurately validate its compliance, or as a result of any data breaches resulting from its storage of Cardholder information. Each party will review and/or monitor the requirements at https:llwww.pcisecuritystandards.org to determine compliance under PCI. As part of this Agreement, Merchant must validate PCI compliance by completion of annual Self Assessment Questionnaires and if applicable, quarterly system scans with an Approved Scanning Vendor as determined by the PCI Security Standards Organization. The foregoing is an ongoing obligation during the term of this Agreement and as it may be renewed. Merchant acknowledges and understands that Merchant may be prohibited from participating in Visa/MasterCard/Discover programs if it is determined that Merchant is noncompliant. The following lists certain of the current PCI requirements, all of which Merchant and Acquirer shall comply with, if applicable: (i) install and maintain a working network firewall to protect data accessible via the Internet; (ii) keep security patches up-to-date;(iii) encrypt stored data; (iv) encrypt data sent across networks; (v) use and regularly update anti-virus software; (vi) restrict access to data to business "need to know," (vii) assign a unique ID to each person with computer access to data; (viii) do not use vendor supplied defaults for system passwords and other security parameters; (ix) track access data by unique ID; (x) maintain a policy that addresses information security for employees and contractors; and (xi) restrict physical access to Cardholder information.

A) Merchant agrees to validate compliance with the requirements of the Payment Card Industry (PCI) Data Security Standards, including, but not limited to, satisfactory completion and submission of Self Assessment Questionnaires (SAQs), and quarterly system scans if determined as necessary by the PCI Data Security Standards on a continual basis. Merchant will be provided with the tools and resources required to complete the validation process. Failure to provide successful PCI validation will cause the Merchant to be subject to a monthly PCI Non Compliance Fee. The PCI Non Compliance fee will be assessed ninety (90) days after approval of Merchant account if merchant has not validated PCI compliance, or after any ninety (90) day consecutive period for which Merchant was not in compliance with validation standards.

B) if (a) a party becomes aware of a breach of the security of its (or its vendors or subcontractors) systems, (b) any Personal Data is disclosed by a party in violation of the Data Protection Standards, or (c) a party becomes aware that an unauthorized access, disclosure or use of such personal data has occurred or is likely to occur as a result of an act or omission of such party or any subcontractor or vendor of such party (each such event, an **"Information Security Breach"**), such party shall immediately notify the other party of such Information Security Breach, and at the discretion of the other party shall promptly: (a) reasonably investigate, remediate, and mitigate the effects of the Information Security Breach and (b) provide the other Party with assurances reasonably satisfactory to such party that such Information Security Breach shall not recur. Additionally, if any Information Security Breach occurs and the Data Protection Standards require notification of public authorities or of individuals whose data was so affected or require other remedial actions, or the other party determines that other remedial measures are warranted, including such party responding to reasonable requests from the other party regarding, and cooperating with the other Party in connection with, any investigation, incident management, media relations or law enforcement activities, and providing consumer remedies such as credit monitoring or ID theft insurance (the foregoing, collectively, the **"Remedial Actions"**), such Party shall, at the other party's request undertake such Remedial Actions or cooperate with the other Party in undertaking Remedial Actions in accordance with industry best practices. For purposes of this Agreement, **"Data Protection Standards"** means Data Protection Laws and Data Security Guidelines; **"Data Protection Laws"** means all federal, state, local laws that pertain to data protection and privacy to the extent such laws are applicable to the activities of the parties under this Agreement; **"Data Security Guidelines"** means all standards, guidelines, practices or procedures required by under applicable laws or regulations or by the payment networks with respect to data security or protection of Personal Data, as such may be amended from time to time, to the extent applicable to the obligations to be performed under this Agreement, including: the Payment Card Industry Data Security Standards ("PCI-DSS") and the PCI Cloud Computing Guidelines; and "Personal Data" means information, data and materials relating to identified or identifiable individuals, including enrollment records, billing and payment records, physical addresses, email addresses, and other personal information, data

March 14, 2023

PR APPROVED:

Exhibit 10P

and materials relating to a party's or its customers, including 'Cardholder Data" (as such term is defined in the Data Security Guidelines).

3.11 Modification

This Agreement is subject to such modifications, changes, and additions as may be required, or deemed by Acquirer to be required by reason of any state or federal statute, judicial decision, Visa/MasterCard/Discover rule or regulation, or the regulation or ruling of any federal agency having jurisdiction over Acquirer or Merchant.

3.12 Changes in Transmission Mode

The means of transmission indicated below shall be the exclusive means utilized by Merchant for the transmission of sales data or credit data to Acquirer. Merchant shall give Acquirer at least thirty (30) days prior written notice of Merchants desire to deliver and deposit actual sales slips and credit slips or otherwise to alter any material in respect to Merchants medium of transmission of sales data and credit data to Acquirer. Following termination, Merchant shall upon request provide Acquirer with all original and microfilm copies required, to be retained as of the date of termination.

3.13 Penalty Fees

A) Acquirer, for the following reasons, may charge a higher discount fee rate on transactions with the following event(s) in accordance with the Visa/MasterCard/Discover published interchange rates:

1) Batches not closed within two (2) business days of the earliest transaction date in the batch;
2) Non-authorized transactions over floor limit;
3) Credit cards not swiped through POS terminal;
4) Terminal did not read the entire content of the magnetic stripe
5) Transaction did not meet Visa/MasterCard/Discover requirements for the best interchange fee.
6) Actual monthly processing volume exceeds approved monthly volume in this Agreement.

3.14 Description of Fees

A) **Discount Fees in accordance with the Visa/MasterCard/Discover published interchange rates**

1) **Retail Qualified Rate:** Swiped consumer credit or check Card transactions that are electronically authorized and closed in a daily batch and include all minimum authorization and transaction information as required for the Visa Custom Payment Service ("CPS") or MasterCard Merit III interchange programs.
2) **MO/TO & Internet Qualified Rate:** Mail Order, Telephone Order or Internet key-entered transaction where the Card is not present and an Address Verification Service is required. Must be a consumer credit or check Card transaction and is electronically authorized and closed in a daily batch and includes all minimum authorization and transaction information as required for CPS Card not Present or CPS Key-Entered or MasterCard Key-Entered interchange programs.
3) **Mid-Qualified (Retail only):** Includes consumer credit and check Card transactions that are a) key-entered, b) not settled within two business days, c) made with cards that have missing or unreadable magnetic stripe or chip data, d) made using a Visa Rewards Card at a T&E Merchant, e) made when the Card is not present.
4) **Non-Qualified (Retail, MO/TO & Internet):** All credit and check Card transactions that do not meet the requirements of the other rate categories. Also includes any transactions made on any Visa Corporate and Signature Card types, MasterCard Commercial or WorldCard Card types or any foreign cards.

3.15 Independent Sales Organization/Member Service Provider

A) Merchant acknowledges that:

1) Acquirer may use an Independent Sales Organization (ISO) or Member Service Provider (MSP) operating under applicable Card Issuer Regulations who is an independent contractor and not an agent of Acquirer,
2) No ISO or MSP has authority to execute this Agreement on Acquirer's behalf or to alter the terms hereof without Acquirer's prior written approval.

3.16 Hold Back

Subsequent to a termination of this Agreement for any reason or upon receipt of actual notice or knowledge that Merchant has or intends to cease operations, Merchant agrees that Acquirer may hold from Merchant's or final settlement amounts a reasonable amount for any items returned, reversed or charged back subsequent to the effective date of termination or cessation of business operations. Acquirer shall forward to Merchant verifications of these items as same are received. Acquirer shall return such withheld amounts to Merchant on the first business day that is ninety (90) days from the effective date of termination, or receipt of notice or knowledge of a location closure as described above.

3.17 General

A) The paragraph headings and captions contained in this agreement are for convenience only, and should not be deemed to define, limit or describe the scope or intent of this agreement to the extent that they conflict with the Substance of this Agreement.

B) This Agreement shall be binding upon and insure to the benefit of the parties hereto and their successors and assigns; provided, however this Agreement may not be assigned by Merchant without the written consent of Acquirer. Any such assignment by Merchant without Acquirer's prior written consent shall be null and void.

C) Should any provision of this Agreement contravene any law, or valid regulation to rule of any regulatory agency of self regulatory body having jurisdiction over either party hereto, or should any provision of this Agreement otherwise be held invalid, or unenforceable by a court or other body of competent jurisdiction, then each such provision shall be automatically terminated and performance hereof by both parties waived, and all other provisions of this Agreement then in effect shall never the less remain in full force and effect.

D) No failure by Acquirer to insist upon strict performance of any term or obligation set forth in this Agreement or to exercise any right or remedy under this Agreement nor acceptance of partial performance during continuance of default hereunder, shall constitute a waiver of any such term, obligation, right or remedy, or a waiver of any such default by Acquirer.

E) Applicable law; venue and mutual jury trial waiver. This Agreement shall be governed and construed exclusively in accordance with the laws of the State of Nevada without reference to its conflicts of laws rules. All of the parties hereto, whether or not actually signatories to this document, agree that the exclusive venue for any and all proceedings relating to this agreement shall be the courts located in the State of Nevada. Furthermore, as material condition to one another in entering into said agreement, each of the parties hereby waive their right to trial by jury in any action or proceeding based upon, arising out of, or in any way relating to this agreement or the relationship between or among said parties, whether sounding in contract or tort or otherwise.

F) All notices or other communications required to be given by either party shall be in writing and shall be effective when hand delivered, emailed, or sent by United States mail, postage prepaid (whether or not sent with a Merchant Statement) and shall be deemed to be given when hand delivered or upon deposit in email or the mail as indicated. Notices shall be addressed to the parties at the address identified below, or such other address as may be specified by either party by notice to the other party.

G) Acquirer may not appoint an Agent(s) to do or take any actions that may be done or taken by Acquirer under this Agreement without Merchant's prior written consent; provided, however, Merchant acknowledges and agrees that it consents to ABC Fitness Solutions, LLC. and/or Trisource Solutions, LLC d/b/a REPAY acting as Agent for Acquirer hereunder. Acquirer shall be responsible for all actions of any approved Agents. Any breach of this Agreement by any Agent of Acquirer (and any act or omission by any Agent of Acquirer that would be a breach of this Agreement if such act or omission were by Acquirer) shall be deemed a breach by Acquirer.

H) This Agreement is intended by the parties as a final expression of and a complete and exclusive statement of the terms of this Agreement there being no conditions to the enforceability of this Agreement. This Agreement may not be amended, supplemented or modified except in writing executed by the parties or unless otherwise provided in this Agreement.

I) Effective date or start date of agreement begins when merchant application is accepted and boarded onto ISO systems. This effective date may vary from merchant acceptance signature date on agreement.

3.18 Electronic Debit/Credit Authorization

Merchant authorizes Acquirer or third party in accordance with this Agreement, to initiate debit/credit entries to Merchant's deposit account, as indicated on Merchant Processing Agreement. This authorization is to remain in full force and effect until:

A) Acquirer has received written notification from Merchant of its termination, in such a manner as to afford Acquirer reasonable opportunity to act on it and

B) All obligations of Merchant to Acquirer that have arisen under this Agreement have been paid in full. This authorization extends, but is not limited, to such entries to this account which concern discount fees, transaction fees, chargebacks, penalties, service fees, return item fees, lease, rental and purchase charges involving Point-Of-Sale ("POS") and credit Card Imprint equipment.

C) Merchant shall regularly and promptly review all statements of account, banking statements, and other communications sent to Merchant and to immediately notify REPAY if any discrepancy exists between Merchant's records and those provided by REPAY, the Merchant's bank, or with respect to any transfer that Merchant believes was not authorized by Merchant or Customer. If Merchant fails to notify REPAY in writing within fourteen (14) calendar days after the date that REPAY mails or otherwise provides a statement of account or other report of activity to Merchant, Merchant will be solely responsible for all losses or other costs associated with any erroneous or unauthorized transfer. The foregoing does not limit in any way Merchant's liability for any breach of this Agreement.

3.19 Representations and Warranties of Merchant

Merchant represents and warrants to Acquirer and REPAY at the time of execution and during the term of this Agreement that:

A) All information contained in the Merchant Application or any other documents delivered to Acquirer and/or REPAY in connection therewith is true and complete and properly reflects Merchant's business, financial condition and principal partners, owners or officers;

B) Merchant has the power to execute, deliver and perform this Agreement, and this Agreement is duly authorized, and does not and will not violate any provisions of Federal or state law or regulation, or conflict with any other agreement to which Merchant is subject;

C) Merchant has all licenses, if any, required to conduct its business and is qualified to do business in every jurisdiction where it is required to do so;

D) There is no action, suit or proceeding now pending or to Merchant's knowledge, threatened by or against or affecting Merchant which would substantially impair its right to carry on its business as now conducted or adversely affect its financial condition or operations;

E) To the best of Merchant's knowledge and belief, each Sales Draft presented to Acquirer for collection is genuine and is not the result of any fraudulent transaction or telemarketing sale or is not being deposited on behalf of any business other than Merchant. Further, Merchant warrants that each Sales Draft is the result of a bona fide Card Transaction for the purchase of goods or services by the Cardholder in the total amount stated on the Sales Draft;

F) Merchant has performed or will perform all of its obligations to the Cardholder in connection with the Card Transaction evidenced thereby;

G) Merchant has complied with Acquirer's and REPAY' procedures for accepting Cards, and the Card Transaction does not involve any element of credit or debit for any purpose other than as set forth in this Agreement and shall not be subject to any defense, dispute, offset or counter claim which may be raised by any Cardholder under the Rules, the Consumer Credit Protection Act (15 USC 1601) or other relevant state or federal statutes or regulations;

H) Any Credit Voucher which it issues represents a bona fide refund or adjustment on a Card sale by Merchant with respect to which a Sales Draft has been accepted;

I) Unless Merchant notifies REPAY in writing (either on the Merchant Application or otherwise), no other processing relationship exists between Merchant and another bankcard processing institution, for this, or any other business run or owned by Merchant.

J) With respect to all Card Transactions that Merchant requests REPAY and Acquirer to originate, Merchant continuously represents and warrants to Acquirer and REPAY that:

1) Each Customer has authorized the debiting and/or crediting of its account;
2) Each Entry is for an amount the customer has agreed to; and
3) Each Entry is in all other respects properly authorized.

3.20 Privacy Policy

This Agreement incorporates by reference our Privacy Policy, which may be found at www.trisourcesolutions.com/privacypolicy.pdf

30187756.1

PR APPROVED:

March 14, 2023

Exhibit 10P

3.21 Definitions

In addition to terms otherwise defined in this Agreement, capitalized terms shall have the meaning ascribed to them in this section.

"Account" means a commercial checking or demand deposit account maintained by Merchant for the crediting of collected funds and the debiting of fees and charges under this Agreement.

"ACH" means the Automated Clearing House paperless entry system controlled by the Federal Reserve Board.

"Agreement" means the Merchant Application, and these Terms and Conditions, and any supplementary documents referenced herein, and schedules, exhibits and amendments to the foregoing.

"American Express" means the Cards bearing the Marks of, and Card Network operated by, American Express Travel Related Services Company, Inc. or its affiliates.

"Authorization" means a computerized function or a direct phone call to a designated number to examine individual Transactions to obtain approval from the Card Issuer to charge the Card for the amount of the sale in accordance with the terms of this Agreement and the Network Rules.

"Bank" has the meaning set forth on the Merchant Application.

"Card" means (i) a valid credit card or debit card in the form issued under license from a Card Network. ("Bank Card"); or (ii) any other valid credit card or debit card or other payment device approved by Bank and accepted by Mer-chant.

"Card Issuer" means the financial institution or company which has provided a Card to a Cardholder.

"Card Network" means Visa U.S.A., Inc., MasterCard International, Inc., American Express Travel Related Services Company, Inc., DFS Services LLC (the owner of Discover) and their affiliates, or any other payment networks approved by Bank that provide Cards accepted by Merchant.

"Card Not Present" or "CNP" means that an Imprint of the Card is not obtained at the point-of-sale.

"Cardholder" (sometimes referred to as "Card Member" in certain Card Network materials) shall mean any person authorized to use the Cards or the accounts established in connection with the Cards.

"Credit Voucher" means a document executed by a Merchant evidencing any refund or price adjustment relating to Cards to be credited to a Cardholder account.

"Discover Card" means a Card bearing the Discover Marks and accepted as part of the DFS Services Network.

"Guarantor" has the meaning set forth on the Merchant Application.

"Guaranty" has the meaning set forth on the Merchant Application.

"ISO" has the meaning set forth on the Merchant Application

"Merchant" has the meaning set forth on the Merchant Application.

"Merchant Application" has the meaning set forth on the Merchant Application.

"Network Rules" means the rules, regulations, releases, interpretations and other requirements (whether contractual or otherwise) imposed or adopted by any Card Networks and related authorities, including without limitation, those of the PCI Security Standards Council, LLC and the National Automated Clearing House Association (including, with respect to EBT, the Quest Operating Rules and with respect to PIN debit cards, the rules, regulations, policies and procedures of the applicable debit network).

"Provider" as provided by the introductory paragraph to these Terms and Conditions, means ISO and Bank together.

"Transaction" means any sale of products or services, or credit for such, from a Merchant for which the Cardholder makes payment through the use of any Card and which is presented to Provider for collection.

"Voice Authorization" means a direct phone call to a designated number to obtain credit approval on a Transaction from the Card Issuer, whether by voice or voice-activated systems.

3.22 Merchant Statement Key

Brand-Originated Fee Names	The names given to particular fees by the card brands (Visa, MasterCard, Discover, American Express)
Statement Fee Names	The names of particular fees as they appear on the repay monthly merchant statement
Fee Descriptions	Explanation/Descriptions of a particular fee

Visa Fee Names	**Statement Names**	**Fee Descriptions**
Visa Auth	Auth fee	Authorization Fee on Visa Transactions
Visa ARU	ARU auth	Authorization Fee for Automated Response Unit on Visa transactions
Visa Voice Auth	Voice auth	Authorization Fee for Voice Authorization on Visa transactions
VISA APF credit	APF credit	Acquiring Processing Fee for Visa Credit Transactions
VISA APF Debit	APF debit	Acquiring Processing Fee for Visa Debit Transactions
VISA Misuse Auth	Misuse auth system	Fee for Misuse of Authorization System on Visa Transactions
Visa FANF	FANF	Fixed Acquirer Network Fee for access to Visa networks
Visa Integrity Fee	Trans Integrity fee	US domestic debit & prepaid card failing CPS qualifications on Visa transactions
Visa Floor Limit Rate	Floor Limit Rate	Transactions without matching authorizations through EQT device on Visa transactions
Visa IAF	IAF	International Acquiring Fee on foreign issued Visa transactions
Visa ISA	ISA	International Service Assessment on Visa transactions
File Transfer	File Transfer	File transfer fee on all Visa transactions
V Excess Att	V Excess Att	Fee for domestic authorization reattempt in excess of 15 within 30 days.
V Excess Att XB	V Excess Att XB	Fee for Cross-Border authorization reattempts in excess of 15 within 30 days.
V High Fallbck	V High Fallbck	Visa Fallback rate of 10% or higher
V AppAtt	V AppAtt	Domestic system integrity fee per transaction assessed for the first and each subsequent reattempt.
V AppAtt Xb	V AppAtt XB	Cross-border system integrity fee per transaction assessed for the first and each subsequent reattempt.
V AVS	V AVS	Assessed per AVS request on all transactions.

MasterCard Fee Names	**Statement Names**	**Fee Descriptions**
MC Auth	Auth fee m	Authorization Fee on MasterCard Transactions
MC ARU	ARU auth m	Authorization Fee for Automated Response Unit on MasterCard transactions
MC Voice Auth	Voice auth m	Authorization Fee for Voice Authorization on MasterCard transactions
MC Misuse Fee	Misuse auth system m	Fee for Misuse of Authorization System on MasterCard Transactions
MC Cross Border/Acq Sup %	Cross Border/Acq Sup	Fees on MasterCard foreign authorizations and/or transactions
MC DEF	DEF	The Digital Enablement Fee will be assessed on all MasterCard card not present sale transactions.
M Acq Merch Advice	M Acq Merch Advice	Fee assessed on CNP where in the past 30 days a transaction on the same card for the same amount is declined with MAC 03 or 21.
MLocation Fee	MLocation Fee	Monthly fee for opened merchants
NABU	NABU	Network Brand Access Usage for MasterCard authorizations
MC Exc Auth	MC Exc Auth	Fee assessed on authorization attempts in excess of 10 declined attempts
MC Decline RC CNP	MC Decline RC CNP	Fee assessed on authorizations processed on MasterCard network where enhanced intelligence is provided

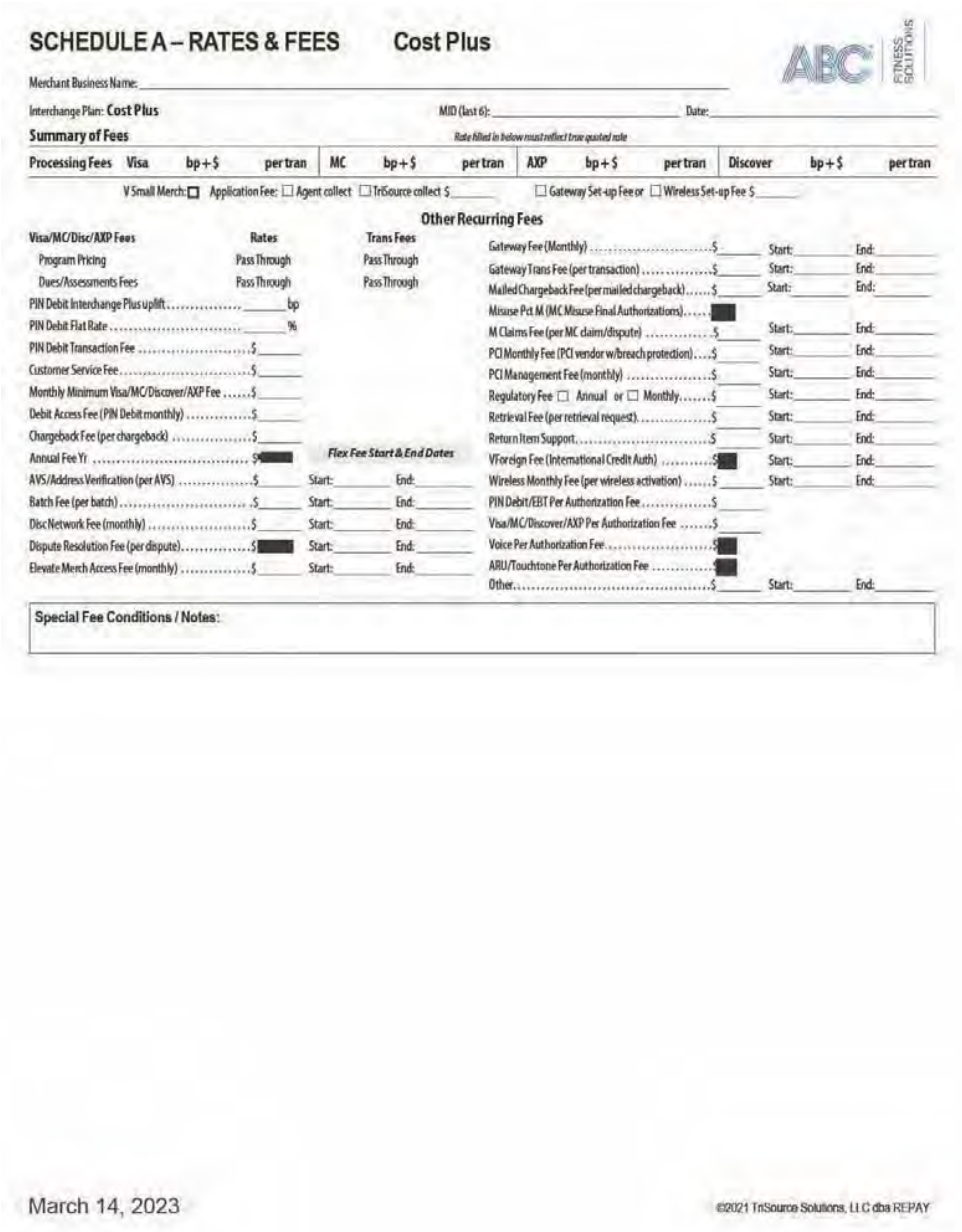
Discover Fee Names	**Statement Names**	**Fee Descriptions**
Discover Network Auth Fee	DNAF	Network Access Fee on Discover Transactions
Disc IPF/ISF	IPF/ISF	International Processing Fee/International Service Fee on Discover foreign transactions
D Trans Integrity	D Trans Integrity	Program Integrity fee applied to all card sales which are submitted at a Mid or Base level program
Disc DUC	DUC	Data Usage Fee on Discover authorizations
Disc Auth	Auth fee d	Authorization Fee on Discover Transactions
Disc ARU	ARU auth d	Authorization Fee for Automated Response Unit on Discover transactions
Disc Voice Auth	Voice auth d	Authorization Fee for Voice Authorization on Discover transactions
D AVS Fee	D AVS Fee	Assessed per AVS request on all transactions
D DigInv Fee	D DigInv Fee	Assessed on gross sales for keyed and ecommerce transactions
D Acct Verify Serv	D Acct Verify Serv	Fee assessed per account verification request

Amex Fee Names	**Statement Names**	**Fee Descriptions**
Assessment Fee	Assessment Fee	The fee applies to gross American Express card volume.
Card-Not-Present Fee	Non-Swiped	The fee applies to gross card-not-present volume, such as keyed and e-commerce transactions. The CNP surcharge is charged in addition to to the sponsorship fee of 0.15%, making the total assessment on card-not-present volume 0.45%.
Inbound Fee	Inbound Fee	The American Express international assessment applies to gross sales volume involving a card issued outside of the United States.
Data Quality Fee	Data Quality Fee	The fee applies to any American Express transaction that does not meet data quality standards, e.g. incorrect MID numbers or incorrect MCCs. The fee is 0.75% of the face amount of the transaction amount.
AcqTran A	AcqTran A	Assessed to all OptBlue US Credit and prepaid transactions. Excludes debit card trans and Refunds
Auth	Auth Fee A	Authorization fee on American Express (AXP) transactions
ARU	ARU auth a	Authorization Fee for Automated Response Unit on AXP authorizations
Voice Auth	Voice auth a	Authorization Fee for Voice Authorization on AXP authorizations
AX OB Pgm Fee	AX OB Pgm Fee	Fees assessed on each AXP OptBlue transaction when AXP volume exceeds $3M.

PR APPROVED:

March 14, 2023

Exhibit 10P



SCHEDULE A – RATES & FEES   Cost Plus

ABC FITNESS SOLUTIONS

Merchant Business Name: ______________________________

Interchange Plan: **Cost Plus**   MID (last 6): ______________ Date: ______________

Summary of Fees   *Rate filled in below must reflect true quoted rate*

Processing Fees	Visa	bp+$	per tran	MC	bp+$	per tran	AXP	bp+$	per tran	Discover	bp+$	per tran

V Small Merch: □   Application Fee: □ Agent collect □ TriSource collect $______   □ Gateway Set-up Fee or □ Wireless Set-up Fee $______

Other Recurring Fees

Visa/MC/Disc/AXP Fees	Rates	Trans Fees
Program Pricing	Pass Through	Pass Through
Dues/Assessments Fees	Pass Through	Pass Through

PIN Debit Interchange Plus uplift................ ______ bp

PIN Debit Flat Rate.............................. ______ %

PIN Debit Transaction Fee........................$______

Customer Service Fee.............................$______

Monthly Minimum Visa/MC/Discover/AXP Fee......$______

Debit Access Fee (PIN Debit monthly)..............$______

Chargeback Fee (per chargeback)..................$______

Annual Fee Yr.....................................$[redacted]

Flex Fee Start & End Dates

AVS/Address Verification (per AVS)................$______ Start: ______ End: ______

Batch Fee (per batch)............................$______ Start: ______ End: ______

Disc Network Fee (monthly)........................$______ Start: ______ End: ______

Dispute Resolution Fee (per dispute)...............$[redacted] Start: ______ End: ______

Elevate Merch Access Fee (monthly)...............$______ Start: ______ End: ______

Gateway Fee (Monthly)..........................$______ Start: ______ End: ______

Gateway Trans Fee (per transaction)...............$______ Start: ______ End: ______

Mailed Chargeback Fee (per mailed chargeback)......$______ Start: ______ End: ______

Misuse Pct M (MC Misuse Final Authorizations)......[redacted]

M Claims Fee (per MC claim/dispute).............$______ Start: ______ End: ______

PCI Monthly Fee (PCI vendor w/breach protection)....$______ Start: ______ End: ______

PCI Management Fee (monthly)...................$______ Start: ______ End: ______

Regulatory Fee □ Annual or □ Monthly.......$______ Start: ______ End: ______

Retrieval Fee (per retrieval request)...............$______ Start: ______ End: ______

Return Item Support.............................$______ Start: ______ End: ______

VForeign Fee (International Credit Auth)...........$[redacted] Start: ______ End: ______

Wireless Monthly Fee (per wireless activation)......$______ Start: ______ End: ______

PIN Debit/EBT Per Authorization Fee...............$______

Visa/MC/Discover/AXP Per Authorization Fee.......$______

Voice Per Authorization Fee.......................$[redacted]

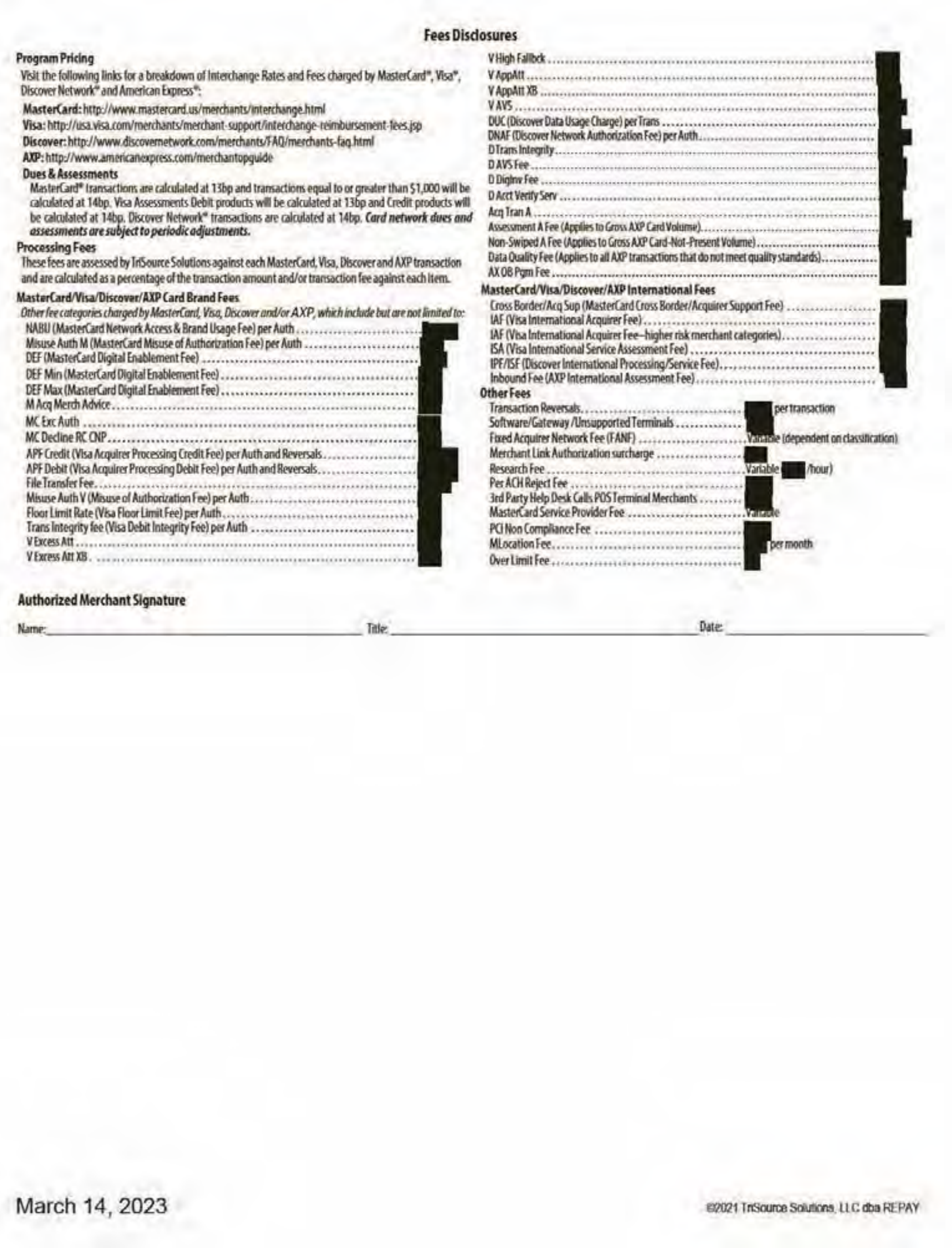
ARU/Touchtone Per Authorization Fee.............$[redacted]

Other..$______ Start: ______ End: ______

Special Fee Conditions / Notes:

March 14, 2023

Exhibit 10P



Fees Disclosures

Program Pricing

Visit the following links for a breakdown of Interchange Rates and Fees charged by MasterCard®, Visa®, Discover Network® and American Express®:

MasterCard: http://www.mastercard.us/merchants/interchange.html
Visa: http://usa.visa.com/merchants/merchant-support/interchange-reimbursement-fees.jsp
Discover: http://www.discovernetwork.com/merchants/FAQ/merchants-faq.html
AXP: http://www.americanexpress.com/merchantopguide

Dues & Assessments

MasterCard® transactions are calculated at 13bp and transactions equal to or greater than $1,000 will be calculated at 14bp. Visa Assessments Debit products will be calculated at 13bp and Credit products will be calculated at 14bp. Discover Network® transactions are calculated at 14bp. ***Card network dues and assessments are subject to periodic adjustments.***

Processing Fees

These fees are assessed by TriSource Solutions against each MasterCard, Visa, Discover and AXP transaction and are calculated as a percentage of the transaction amount and/or transaction fee against each item.

MasterCard/Visa/Discover/AXP Card Brand Fees

Other fee categories charged by MasterCard, Visa, Discover and/or AXP, which include but are not limited to:

NABU (MasterCard Network Access & Brand Usage Fee) per Auth	[redacted]
Misuse Auth M (MasterCard Misuse of Authorization Fee) per Auth	[redacted]
DEF (MasterCard Digital Enablement Fee)	[redacted]
DEF Min (MasterCard Digital Enablement Fee)	[redacted]
DEF Max (MasterCard Digital Enablement Fee)	[redacted]
M Acq Merch Advice	[redacted]
MC Exc Auth	[redacted]
MC Decline RC CNP	[redacted]
APF Credit (Visa Acquirer Processing Credit Fee) per Auth and Reversals	[redacted]
APF Debit (Visa Acquirer Processing Debit Fee) per Auth and Reversals	[redacted]
File Transfer Fee	[redacted]
Misuse Auth V (Misuse of Authorization Fee) per Auth	[redacted]
Floor Limit Rate (Visa Floor Limit Fee) per Auth	[redacted]
Trans Integrity fee (Visa Debit Integrity Fee) per Auth	[redacted]
V Excess Att	[redacted]
V Exress Att XB	[redacted]
V High Fallbck	[redacted]
V AppAtt	[redacted]
V AppAtt XB	[redacted]
V AVS	[redacted]
DUC (Discover Data Usage Charge) per Trans	[redacted]
DNAF (Discover Network Authorization Fee) per Auth	[redacted]
D Trans Integrity	[redacted]
D AVS Fee	[redacted]
D DigInv Fee	[redacted]
D Acct Verify Serv	[redacted]
Acq Tran A	[redacted]
Assessment A Fee (Applies to Gross AXP Card Volume)	[redacted]
Non-Swiped A Fee (Applies to Gross AXP Card-Not-Present Volume)	[redacted]
Data Quality Fee (Applies to all AXP transactions that do not meet quality standards)	[redacted]
AX OB Pgm Fee	[redacted]

MasterCard/Visa/Discover/AXP International Fees

Cross Border/Acq Sup (MasterCard Cross Border/Acquirer Support Fee)	[redacted]
IAF (Visa International Acquirer Fee)	[redacted]
IAF (Visa International Acquirer Fee–higher risk merchant categories)	[redacted]
ISA (Visa International Service Assessment Fee)	[redacted]
IPF/ISF (Discover International Processing/Service Fee)	[redacted]
Inbound Fee (AXP International Assessment Fee)	[redacted]

Other Fees

Transaction Reversals	[redacted] per transaction
Software/Gateway /Unsupported Terminals	[redacted]
Fixed Acquirer Network Fee (FANF)	Variable (dependent on classification)
Merchant Link Authorization surcharge	[redacted]
Research Fee	Variable [redacted] /hour)
Per ACH Reject Fee	[redacted]
3rd Party Help Desk Calls POS Terminal Merchants	[redacted]
MasterCard Service Provider Fee	Variable
PCI Non Compliance Fee	[redacted]
MLocation Fee	[redacted] per month
Over Limit Fee	[redacted]

Authorized Merchant Signature

Name: ______________________ Title: ______________________ Date: ______________________

March 14, 2023

Exhibit 10S

FRANCHISE DISCLOSURE DOCUMENT

Planet Fitness Franchising LLC
(a Delaware Limited Liability Company)
4 Liberty Lane West, Floor 2
Hampton, NH 03842
(603) 750-0001
www.planetfitness.com

PLANET FITNESS® businesses are fitness training facilities offering exercise machines and free weights, fitness training services, related services, amenities, and ancillary goods. We offer for sale **PLANET FITNESS** franchises for new locations and for existing fitness facilities that want to convert to a **PLANET FITNESS**.

The total investment necessary to begin operation of a single **PLANET FITNESS®** facility ranges from $1,504,600 to $3,691,500 if you finance your equipment. This includes $43,000 to $352,000 that must be paid to the franchisor or its affiliate. If you choose to purchase your equipment, the total investment necessary to begin operation of a single **PLANET FITNESS®** facility ranges from $2,579,600 to $5,158,500. This includes $425,000 to $1,093,000 that must be paid to the franchisor or its affiliate. These estimated initial investment ranges also apply to each location that you develop under the Area Development Agreement (plus the Area Development Fee you pay at the time you sign the Area Development Agreement). If you sign an Area Development Agreement, you must develop one or more **PLANET FITNESS®** facilities, and you will pay an Area Development Fee of $10,000 per planned location (paid in full when you sign the Area Development Agreement) in addition to the then-current initial franchise fee due for each location at the time the Franchise Agreement for that location is signed.

This Disclosure Document summarizes certain provisions of your franchise agreement and other information in plain English. Read this Disclosure Document and all accompanying agreements carefully. You must receive this Disclosure Document at least 14 calendar days before you sign a binding agreement with, or make any payment to, us or an affiliate in connection with the proposed franchise sale. **Note, however, that no government agency has verified the information contained in this document.**

You may wish to receive your Disclosure Document in another format that is more convenient for you. To discuss the availability of disclosures in different formats, contact Jason Bauman, Associate General Counsel, Franchising, at 4 Liberty Lane West, Hampton, NH 03842 and (603) 750-0001.

The terms of your contract will govern your franchise relationship. Don't rely on the Disclosure Document alone to understand your contract. Read all of your contract carefully. Show your contract and this Disclosure Document to an advisor, like a lawyer or accountant.

Buying a franchise is a complex investment. The information in this Disclosure Document can help you make up your mind. More information on franchising, such as "A Consumer's Guide to Buying a Franchise," which can help you understand how to use this Disclosure Document, is available from the Federal Trade Commission. You can contact the FTC at 1-877-FTC-HELP or by writing to the FTC at 600 Pennsylvania Avenue NW, Washington, DC 20580. You can also visit the FTC's home page at www.ftc.gov for additional information on franchising.

There may also be laws on franchising in your state. Ask your state agencies about them.

Issuance date: June 5, 2024

Exhibit 10T

ADDENDUM TO **PLANET FITNESS®** DISCLOSURE DOCUMENT FOR THE STATE OF MARYLAND

The following applies to franchises and franchisees subject to Maryland statutes and regulations. Item numbers correspond to those in the main body:

No statement, questionnaire, or acknowledgment signed or agreed to by you in connection with the commencement of the franchise relationship shall have the effect of (i) waiving any claims under any applicable state franchise law, including fraud in the inducement, or (ii) disclaiming reliance on any statement made by any franchisor, franchise seller, or other person acting on behalf of the Franchisor. This provision supersedes any other term of any document executed in connection with the franchise.

Item 5.

Item 5 is supplemented by the addition of the following language:

"We will defer collection from you of the Initial Franchise Fee and any other fees due to us from you before the opening of your Planet Fitness location, until we have completed our pre-opening obligations to you under the Franchise Agreement.

We will defer collection from you of the Area Development Fee and any other fees due to us from you before the opening of our Planet Fitness area development business, until we have completed our pre-opening obligations to you under the Area Development Agreement."

Item 8.

Item 8 is supplemented by the addition of the following language:

"Our affiliate, Planet Fitness Distribution LLC ("PF Equipment"), is the sole distributor of fitness equipment for your Business. PF Equipment's costs for the equipment include the cost of salaries and commission payments, administrative costs and profit. We believe the amounts you pay PF Equipment for these products is approximately equal to or less than the prevailing market price you would pay if you purchased fitness equipment of a comparable quality (including with respect to extended warranties and unique branding applications) from a third-party.

If PF Equipment is no longer able to provide you with fitness equipment, we will endeavor to provide such equipment through one or more alternate suppliers at comparable cost."

Item 17.

1. Any claims arising under the Maryland Franchise Registration and Disclosure law must be brought within 3 years after we grant you a **PLANET FITNESS®** franchise.

Exhibit 10T

2. Our termination of the Franchise Agreement because of your bankruptcy may not be enforceable under applicable federal law (11 U.S.C.A. 101 et seq.)

3. Any claims under the Maryland Franchise Registration and Disclosure law may be brought in the State of Maryland.

4. Pursuant to COMAR 02.02.0816L, the general release required as a condition of renewal and/or assignment/transfer will not apply to any liability under the Maryland Franchise Registration and Disclosure Law.

Each provision of this Addendum shall be effective only to the extent that, with respect to such provision, the jurisdictional requirements of the Maryland Franchise Registration and Disclosure Law are met independently without reference to this Addendum.

Exhibit 10T

AMENDMENT TO **PLANET FITNESS®** FRANCHISE AGREEMENT FOR THE STATE OF MARYLAND

Notwithstanding anything which may be contained in the body of the Franchise Agreement to the contrary, the Franchise Agreement is amended as follows:

1. Section 1.2 of the Franchise Agreement shall be deleted in its entirety and replaced with the following language:

> You acknowledge that, in all of their dealings with you, our officers, directors, employees and agents act only in a representative, and not in an individual, capacity. All business dealing between you and such persons as a result of this Agreement are solely between you and us.

2. The second to last sentence of Section 4.1 of the Franchise Agreement is hereby deleted in its entirety.

3. Article 5.1 (Initial Franchise Fee) is amended to provide that we will defer collection of the Initial Franchise Fee and any other fees you owe us under the Franchise Agreement before your **PLANET FITNESS®** business opens, until we have completed our initial obligations to you under the Franchise Agreement.

4. Article 19.11 (Consent to Jurisdiction) is amended to provide that you may bring a lawsuit in Maryland for claims arising under the Maryland Franchise Registration and Disclosure Law.

5. The two paragraphs immediately preceding the "[FRANCHISEE]" signature block of the Franchise Agreement are hereby deleted in their entirety.

6. Any claims arising under the Maryland Franchise Registration and Disclosure Law must be brought within three years after the date of the Franchise Agreement.

7. No statement, questionnaire, or acknowledgment signed or agreed to by Franchisee in connection with the commencement of the franchise relationship shall have the effect of (i) waiving any claims under any applicable state franchise law, including fraud in the inducement, or (ii) disclaiming reliance on any statement made by any franchisor, franchise seller, or other person acting on behalf of the Franchisor. This provision supersedes any other term of any document executed in connection with the franchise.

8. Pursuant to COMAR 02.02.08.16L, the general release required as a condition of renewal, assignment or transfer will not apply to any liability under the Maryland Franchise Registration and Disclosure law.

Exhibit 10T

Each provision of this Amendment is effective only to the extent, with respect to such provision, that the jurisdictional requirements of the Maryland Franchise Registration and Disclosure Law are met independently without reference to this Amendment.

Each of the undersigned hereby acknowledges having read and understood this Amendment and consents to be bound by all of its terms.

IN WITNESS WHEREOF, the parties hereto have duly executed this Amendment to the Franchise Agreement as of the Effective Date of the Franchise Agreement.

[FRANCHISEE]	PLANET FITNESS FRANCHISING LLC
By: ______________________ (Authorized Representative)	By: ______________________
Print Name:______________________	Print Name: Justin Vartanian
Title: ______________________	Title: General Counsel and SVP, International Division

Exhibit 10U

ADDENDUM TO
PLANET FITNESS®
DISCLOSURE DOCUMENT FOR THE
STATE OF CALIFORNIA

The following information applies to franchises and franchisees subject to the California Franchise Investment Act. Item numbers correspond to those in the main body:

THE CALIFORNIA FRANCHISE INVESTMENT LAW REQUIRES THAT A COPY OF ALL PROPOSED AGREEMENTS RELATING TO THE SALE OF THE FRANCHISE BE DELIVERED TOGETHER WITH THE DISCLOSURE DOCUMENT.

THESE FRANCHISES WILL BE/HAVE BEEN REGISTERED (OR EXEMPT FROM REGISTRATION) UNDER THE FRANCHISE INVESTMENT LAW OF THE STATE OF CALIFORNIA. SUCH REGISTRATION DOES NOT CONSTITUTE APPROVAL, RECOMMENDATION, OR ENDORSEMENT BY THE COMMISSIONER OF FINANCIAL PROTECTION AND INNOVATION NOR A FINDING BY THE COMMISSIONER THAT THE INFORMATION PROVIDED HEREIN IS TRUE, COMPLETE, AND NOT MISLEADING.

OUR WEBSITE HAS NOT BEEN REVIEWED OR APPROVED BY THE CALIFORNIA DEPARTMENT OF FINANCIAL PROTECTION AND INNOVATION. ANY COMPLAINTS CONCERNING THE CONTENT OF THIS WEBSITE MAY BE DIRECTED TO THE CALIFORNIA DEPARTMENT OF FINANCIAL PROTECTION AND INNOVATION AT www.dfpi.ca.gov.

Before the franchisor can ask you to materially modify your existing franchise agreement, Section 31125 of the California Corporations Code requires the franchisor to file a material modification application with the Department that includes a disclosure document showing the existing terms and the proposed new terms of your franchise agreement. Once the application is registered, the franchisor must provide you with that disclosure document with an explanation that the changes are voluntary.

No statement, questionnaire, or acknowledgment signed or agreed to by you in connection with the commencement of the franchise relationship shall have the effect of (i) waiving any claims under any applicable state franchise law, including fraud in the inducement, or (ii) disclaiming reliance on any statement made by any franchisor, franchise seller, or other person acting on behalf of the Franchisor. This provision supersedes any other term of any document executed in connection with the franchise.

Item 3.

Item 3 is amended to provide that neither we nor any other person identified in Item 2 is subject to any currently effective order of any national securities association or national securities exchange, as defined in the Securities Exchange Act of 1934, 15 U.S.C. 78a et seq., suspending or expelling such persons from membership in such association or exchange.

Exhibit 10U

Item 6.

Item 6, under the heading entitled "Interest," shall be amended to provide that the highest interest rate allowed by law in California is ten percent (10%).

Item 17.

1. California Business & Professions Code Sections 20000 through 20043 provide rights to you concerning termination, transfer, or nonrenewal of a franchise. If the Franchise Agreement contains a provision that is inconsistent with the law, the law will control.

2. Termination of the Franchise Agreement by us because of your insolvency or bankruptcy may not be enforceable under applicable federal law (11 U.S.C.A. 101 et seq.).

3. The Franchise Agreement contains a covenant not to compete which extends beyond the termination of the franchise. This provision may not be enforceable under California law.

4. You must sign a general release if you are granted a successor franchise or transfer your franchise. These provisions may be unenforceable under California law. California Corporations Code 31512 voids a waiver of your rights under the Franchise Investment Law (California Corporations Code 31000 through 31516). Business and Professions Code 20010 voids a waiver of your rights under the Franchise Relations Act (Business and Professions Code 20000 through 20043).

5. The Franchise Agreement requires the application of the laws of New Hampshire. This provision may not be enforceable under California law.

6. The Franchise Agreement requires binding arbitration. The arbitration will occur in Portsmouth, New Hampshire (or the in the city of our then-current headquarters).

7. Prospective franchisees are encouraged to consult private legal counsel to determine the applicability of California and federal laws (such as Business and Professions Code Section 20040.5, Code of Civil Procedure Section 1281, and the Federal Arbitration Act) to any provisions of a franchise agreement restricting venue to a forum outside the State of California.

8. The Franchise Agreement contains a waiver of punitive damages provision, which may not be enforceable.

Each provision of this Addendum to the Franchise Disclosure Document shall be effective only to the extent that with respect to such provision, the jurisdictional requirements of the California Franchise Investment Law are met independently without reference to this Addendum.

Exhibit 10U

AMENDMENT TO **PLANET FITNESS®** FRANCHISE AGREEMENT FOR THE STATE OF CALIFORNIA

Notwithstanding anything which may be contained in the body of the Franchise Agreement to the contrary, the Franchise Agreement is amended to include the following:

1. The Franchise Agreement contains a covenant not to compete which extends beyond the term of the franchise. This provision may not be enforceable under California law.

2. The Franchise Agreement requires the application of the laws of New Hampshire. This provision may not be enforceable under California law.

3. The Franchise Agreement gives us the right to terminate the Franchise Agreement in the event of Franchisee's bankruptcy. This provision may not be enforceable under federal bankruptcy laws (11 U.S.C. Section 101, et seq.).

4. Any and all provisions of the Franchise Agreement that provide for periods of notice less than those required by California law, or provide for transfer, termination, cancellation, nonrenewal, or the like other than in accordance with California law, shall, to the extent such are not in accordance with California law, be superseded by said law.

5. Section 1.2 of the Franchise Agreement shall be deleted in its entirety and replaced with the following language:

> You acknowledge that, in all of their dealings with you, our officers, directors, employees and agents act only in a representative, and not in an individual, capacity. All business dealing between you and such persons as a result of this Agreement are solely between you and us.

6. The second to last sentence of Section 4.1 of the Franchise Agreement is hereby deleted in its entirety.

7. The two paragraphs immediately preceding the "[FRANCHISEE]" signature block of the Franchise Agreement are hereby deleted in their entirety.

8. No statement, questionnaire, or acknowledgment signed or agreed to by Franchisee in connection with the commencement of the franchise relationship shall have the effect of (i) waiving any claims under any applicable state franchise law, including fraud in the inducement, or (ii) disclaiming reliance on any statement made by any franchisor, franchise seller, or other person acting on behalf of the Franchisor. This provision supersedes any other term of any document executed in connection with the franchise.

9. Each provision of this Amendment shall be effective only to the extent, with respect to such provision, that the jurisdictional requirements of the California Franchise Investment Law and California Franchise Relations Act are met independently without reference to this Amendment.

Exhibit 10U

10. In all other respects, the Franchise Agreement will be construed and enforced according to its terms.

Each of the undersigned hereby acknowledges having read and understood this Amendment and consents to be bound by all of its terms.

IN WITNESS WHEREOF, the parties hereto have duly executed this Amendment to the Franchise Agreement as of the Effective Date of the Franchise Agreement.

[FRANCHISEE]	PLANET FITNESS FRANCHISING LLC
By: ________________________ (Authorized Representative)	By: ________________________
Print Name:____________________	Print Name: Justin Vartanian
Title: ________________________	Title: General Counsel and SVP, International Division

Exhibit 10U

AMENDMENT TO
PLANET FITNESS®
AREA DEVELOPMENT AGREEMENT FOR THE
STATE OF CALIFORNIA

Notwithstanding anything which may be contained in the body of the Area Development Agreement to the contrary, the Area Development Agreement is amended to include the following:

1. The Area Development Agreement contains a covenant not to compete which may extend beyond the term of the franchise. This provision may not be enforceable under California law.

2. The Area Development Agreement requires the application of the laws of New Hampshire. This provision may not be enforceable under California law.

3. Any and all provisions of the Area Development Agreement that provide for periods of notice less than those required by California law, or provide for transfer, termination, cancellation, nonrenewal, or the like other than in accordance with California law, shall, to the extent such are not in accordance with California law, be superseded by said law.

4. The two paragraphs immediately preceding the "[AREA DEVELOPER]" signature block of the Franchise Agreement are hereby deleted in their entirety.

5. No statement, questionnaire, or acknowledgment signed or agreed to by a franchisee in connection with the commencement of the franchise relationship shall have the effect of (i) waiving any claims under any applicable state franchise law, including fraud in the inducement, or (ii) disclaiming reliance on any statement made by any franchisor, franchise seller, or other person acting on behalf of the Franchisor. This provision supersedes any other term of any document executed in connection with the franchise.

6. Each provision of this Amendment shall be effective only to the extent, with respect to such provision, that the jurisdictional requirements of the California Franchise Investment Law and California Franchise Relations Act are met independently without reference to this Amendment.

7. In all other respects, the Area Development Agreement will be construed and enforced according to its terms.

Exhibit 10U

Each of the undersigned hereby acknowledges having read and understood this Amendment and consents to be bound by all of its terms.

IN WITNESS WHEREOF, the parties hereto have duly executed this Amendment to the Area Development Agreement as of the Effective Date of the Area Development Agreement.

[AREA DEVELOPER]	PLANET FITNESS FRANCHISING LLC
By: ______________________________ (Authorized Representative)	By: ______________________________
Print Name:______________________________	Print Name: Justin Vartanian
Title: ______________________________	Title: General Counsel and SVP, International Division

Exhibit 10V

S E

The following states have franchise laws that require that the Franchise Disclosure Document be registered or filed with the state, or be exempt from registration: California, Hawaii, Illinois, Indiana, Maryland, Michigan, Minnesota, New York, North Dakota, Rhode Island, South Dakota, Virginia, Washington, and Wisconsin.

This document is effective and may be used in the following states, where the document is filed, registered or exempt from registration, as of the Effective Date stated below:

S	**E**
California	June 5, 2024
Illinois	June 5, 2024
Indiana	Pending
Maryland	Pending
Michigan	June 5, 2024
Minnesota	Pending
New York	June 5, 2024
North Dakota	Pending
Rhode Island	Pending
South Dakota	Pending
Virginia	Pending
Washington	See Separate FDD
Wisconsin	June 6, 2024

Other states may require registration, filing, or exemption of a franchise under other laws, such as those that regulate the offer and sale of business opportunities or seller-assisted marketing plans.

Exhibit 10V

RE EIPT

This Disclosure Document summarizes certain provisions of the franchise agreement and other information in plain language. Read this Disclosure Document and all agreements carefully.

If Planet Fitness Franchising LLC offers you a franchise, it must provide this Disclosure Document to you 14 calendar days before you sign a binding agreement with, or make a payment to, us or an affiliate in connection with the proposed franchise sale.

Michigan requires that Planet Fitness Franchising LLC give you this Disclosure Document at least 10 business days before the execution of any binding franchise or other agreement or the payment of any consideration, whichever occurs first.

If Planet Fitness Franchising LLC does not deliver this Disclosure Document on time or if it contains a false or misleading statement, or a material omission, a violation of federal law and state law may have occurred and should be reported to the Federal Trade Commission, Washington, D.C. 20580 and the appropriate state agency identified on Exhibit A.

Planet Fitness Franchising LLC authorizes the agents listed in Exhibit A to receive service of process on its behalf.

The name, principal business address, and telephone number of each franchise seller offering the franchise is:

□ Sara Grotheer, 4 Liberty Lane West, Hampton, NH 03842, (603) 750-0001

□ ______________________________

Issuance Date: June 5, 2024

I have received a Disclosure Document dated June 5, 2024 that included the following Exhibits:

A. List of State Agencies and Agents to Receive Service of Process
B. Nondisclosure & Non-Use Agreement
C. Franchise Agreement (including Addenda and Appendices)
D. Acquisition Amendment to Franchise Agreement
E. Successor Amendment to Franchise Agreement
F. Conversion Amendment to Franchise Agreement
G. Area Development Agreement (including Addenda and Appendices)
H. Financial Statements
I. List of Franchise and Corporate Locations
J. Form of General Release
K-1. Equipment Terms
K-2. Co-op Bylaws
K-3. Voluntary Marketing Pilot Participation Amendment
K-4. POS Agreements
L. Table of Contents to Operations Manual
M. State Addenda

______________	______________________________	______________________
Date	Signature	Printed Name
______________	______________________________	______________________
Date	Signature	Printed Name

Please sign this copy of the receipt, date your signature, and keep it for your records.

P F

Exhibit 10V

RE EIPT

This Disclosure Document summarizes certain provisions of the franchise agreement and other information in plain language. Read this Disclosure Document and all agreements carefully.

If Planet Fitness Franchising LLC offers you a franchise, it must provide this Disclosure Document to you 14 calendar days before you sign a binding agreement with, or make a payment to, us or an affiliate in connection with the proposed franchise sale.

Michigan requires that Planet Fitness Franchising LLC give you this Disclosure Document at least 10 business days before the execution of any binding franchise or other agreement or the payment of any consideration, whichever occurs first.

If Planet Fitness Franchising LLC does not deliver this Disclosure Document on time or if it contains a false or misleading statement, or a material omission, a violation of federal law and state law may have occurred and should be reported to the Federal Trade Commission, Washington, D.C. 20580 and the appropriate state agency identified on Exhibit A.

Planet Fitness Franchising LLC authorizes the agents listed in Exhibit A to receive service of process on its behalf.

The name, principal business address, and telephone number of each franchise seller offering the franchise is:

□ Sara Grotheer, 4 Liberty Lane West, Hampton, NH 03842, (603) 750-0001

□ ____

Issuance Date: June 5, 2024

I have received a Disclosure Document dated June 5, 2024 that included the following Exhibits:

A. List of State Agencies and Agents to Receive Service of Process
B. Nondisclosure & Non-Use Agreement
C. Franchise Agreement (including Addenda and Appendices)
D. Acquisition Amendment to Franchise Agreement
E. Successor Amendment to Franchise Agreement
F. Conversion Amendment to Franchise Agreement
G. Area Development Agreement (including Addenda and Appendices)
H. Financial Statements
I. List of Franchise and Corporate Locations
J. Form of General Release
K-1. Equipment Terms
K-2. Co-op Bylaws
K-3. Voluntary Marketing Pilot Participation Amendment
K-4. POS Agreements
L. Table of Contents to Operations Manual
M. State Addenda

____________	______________________________	______________________
Date	Signature	Printed Name
____________	______________________________	______________________
Date	Signature	Printed Name

Please sign this copy of the receipt, date your signature, and return it to Manager of Business Development,
4 Liberty Lane West, Floor 2, Hampton, NH

F

4885-0250-2592, v. 2

Exhibit 10B

From: Ryan Wagner
To: Glenn Norris; Justin Drummond
Subject: RE: 12 July 2023 - Notes
Date: Friday, July 14, 2023 9:06:32 AM
Attachments: image002.png
image008.png
image009.png
image010.png
image011.png
image012.png
image013.png
ohanagrowthpartnersfinallogo_7fa8dba2-2909-40ee-839a-12ba06da3de6.png

Will do, thank you.

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Friday, July 14, 2023 8:58 AM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>; Justin Drummond <Justin.Drummond@ohanagp.com>
Subject: RE: 12 July 2023 - Notes

OK, make sure it is approved before making any final commitments. Thank you, Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Friday, July 14, 2023 8:33 AM
To: Glenn Norris <glenn@ohanagp.com>; Justin Drummond <Justin.Drummond@ohanagp.com>
Subject: RE: 12 July 2023 - Notes

Absolutely, We are in the RFS process. Once I have vendor selection finalized, I will complete an analysis to discuss.

Ryan Wagner

Exhibit 10B

Vice President of IT
Ohana Growth Partners, LLC

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Friday, July 14, 2023 8:19 AM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>; Justin Drummond <Justin.Drummond@ohanagp.com>
Subject: RE: 12 July 2023 - Notes

Ryan, please go into detail with current cost vs new costs with me.

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Friday, July 14, 2023 8:01 AM
To: Glenn Norris <glenn@ohanagp.com>; Justin Drummond <Justin.Drummond@ohanagp.com>
Subject: RE: 12 July 2023 - Notes

We didn't go into this too much detail yesterday.

Phase 1 - 3 ETA is end of Q1 2024.

- VoIP price increases puts us post Dec 31
- Jan/Feb lock down puts us in March

Phase 1: Logically and OGP are taking over OGP and HQ device management.

- Marc is being told that it is to help Logically best manage the clubs, and I want to manage the HQ.
- Status: In Progress – ETA is weeks

Phase 2: Logically is replacing all of the WiFi at OGP Clubs

- Marc is being told that this is because of the PFHQ mandate
- Status: In Progress – ETA 15 November for most clubs – A few OSI are doing in December.

Phase 3: VoIP

- Options are being explored and prices gathered.
  - Plan is to cut over AFTER Jan 1 because this will be a decent jump in OpEx cost because Marc doesn't charge us anywhere near market rate.
- Status: RFS

Phase 4: BB Clubs

- Despite everything, Marc does provide value at the right price for BB.
- Status: TBD

Exhibit 10B

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Thursday, July 13, 2023 9:31 AM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>; Justin Drummond <Justin.Drummond@ohanagp.com>
Subject: RE: 12 July 2023 - Notes

Ryan, all the attachments are real good if utilized and completed to your satisfaction with the highest quality and timeliness executed . The summary below clearly states you are not satisfied with Marc Radik. You need to have the best internal and external team supporting you. Please explain to me at our 2PM call today your plan to make your desired changes. Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Thursday, July 13, 2023 12:28 AM
To: Justin Drummond <Justin.Drummond@ohanagp.com>; Glenn Norris <glenn@ohanagp.com>
Subject: FW: 12 July 2023 - Notes

The executive summary of this email:

- I am on top of it – you do not need to read the email.
    - I am providing it to you for transparency. Part of my response gives a timeline of events I generated from emails and notes. While writing it, I read emails and notes that reminded me of key elements about our journey. Considering the recent events with Josh/Development – I believe the reminder and context of the journey is imperative.

A Little More Info:

- Marc continues to provide more examples of how he does NOT:
    - Know the PFHQ standards
    - Understand the technology he is installing
- This thread started as a reminder to Marc because he told me he would do something and then did not.
    - The pattern of feedback I have received about Marc from our vendors and partners is summed up as "Marc

Exhibit 10B

believes he knows best and does what he believes is best."

- Every step of Reisterstown has matched this pattern where I tell him to do X, Y, and Z --- he does H, Q, and V.
- When I follow up with him, the gist of what he says is -- "It's better this way" or "It's the same thing." – it is not.

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

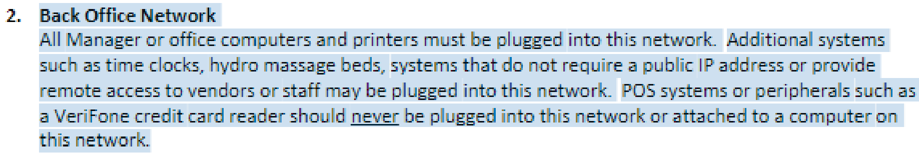
From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Thursday, July 13, 2023 12:06 AM
To: Marc Radik <mjradik@fusedtech.com>; Andrew Dinh <adinh@osisupport.com>; Logan Ford <lford@osisupport.com>; Colin Lucena <clucena@osisupport.com>
Cc: ITO <ito@ohanagp.com>
Subject: RE: 12 July 2023 - Notes

@Andrew Dinh @Colin Lucena @Logan Ford Please read this as well to understand the history of how we arrived here and hopefully appreciate and understand the gravity of the situation.

@Andrew Dinh As the IT Installer on record, we should discuss this offline.

@Marc Radik
On Rockbot – I will dig into it deeper because on Monday, I looked with Logan and verified that two players were currently offline, with a total of 5, and both were offline for less than the time of the remodel, which is where we obtained the data. However, the Rockbot power currently shows the 5th player as unprovisioned to the PE@PF. In cases where a 5th player was not assigned to a normal zone – it followed the PFHQ rule set for secondary placement. I can provide an update once I find out why things changed in the dashboard.

On T-Max –There was an older T-Max solution that connected directly to a control panel. That system was replaced before 2020 and replaced with a new system that uses our network. For all OGP clubs, they have been connected to our Back Office network physically, and this meets PFHQ standards.



2. **Back Office Network**
All Manager or office computers and printers must be plugged into this network. Additional systems such as time clocks, hydro massage beds, systems that do not require a public IP address or provide remote access to vendors or staff may be plugged into this network. POS systems or peripherals such as a VeriFone credit card reader should never be plugged into this network or attached to a computer on this network.

Recently, Merlowe wanted to move one of those to a wireless network because the cables kept being damaged and that led us to have a deeper conversation with logically as to what wifi network that needs to be on. If we want to connect wirelessly – they need to go on the Secure Vendor Network, not to be confused with the vlan40 vendor network, because of the type of traffic that is used to manage the T-max units.

Exhibit 10B

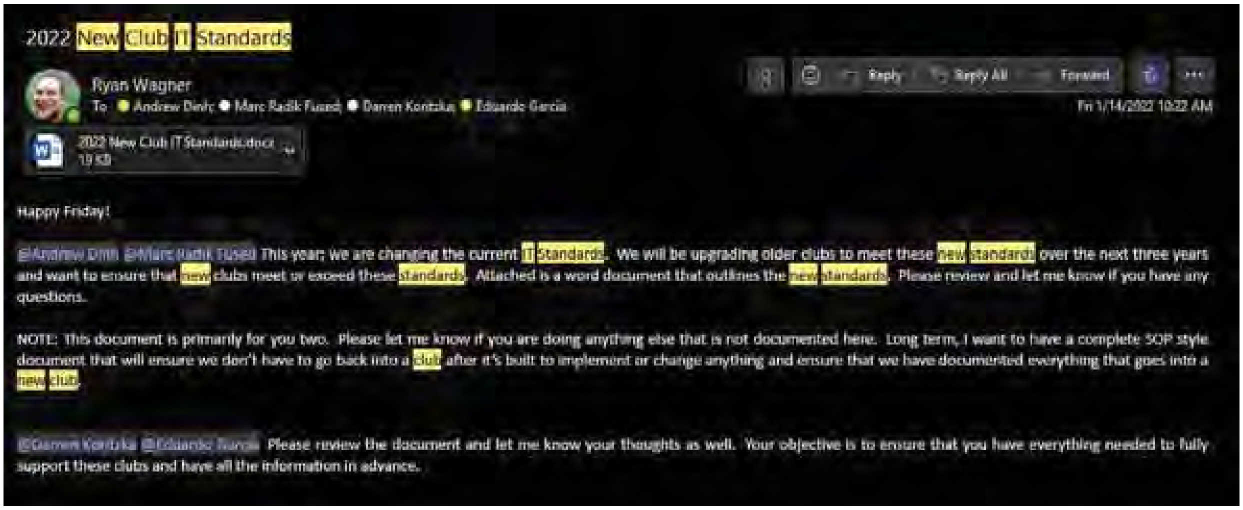
5. **Secure Vendor Network**
   This wireless network is designated for Radianse hardware and other PCI/secure vendor-based equipment. There is a required SSID and configuration. Please work with your mandatory Wi-Fi vendor for more detail.

There are 5 WiFI networks all of clubs should have per PFHQ standards:

- VLAN 10: POS iPad Kiosk
  - This is a PCI compliance network that connects the iPads
- VLAN 20: Back Office
  - Restricted to OGP-owned devices that do not require a different network.
- VLAN 30: Member/Guest
  - Lots of outbound access, access to anything else is completely blocked
- VLAN 40: Vendor Equipment
  - Lifetime, Matrix, etc. – No Authentication or Sensitive Data Traffic
- VLAN 50: Secure Vendor
  - Vendor Equipment that transmits sensitive data or passes authentication. If there is a management device/kiosk that device must use a specific IP.

I started with OGP in February 2020. On January 6, 2021, Josh Beyer was notified by PFHQ that Olympia and Seattle, WA, had failed assessments due to wifi compliance using v4.0 of the PFHQ standards documentation. This was when I became involved for the first time. I followed up with Steve Dalgar to work out a plan which resulted in a temporary exemption and protected us from more severe ramifications. Throughout 2021 we were found to have numerous compliance violations, and I followed up with you and Andrew about it numerous times by phone and email. This continued into December of 2021, with all three of us discussing details about the then-current PF Club IT and Network requirements v4.1 document, but it did not result in those standards being implemented. This resulted in Cielo being awarded Delray, and Delray was the only club that passed compliance without an issue from HQ that year. However, Development wanted to utilize you and Andrew, so we agreed that I would prepare a document for you to follow, and OGP Development would ensure that things met PFHQ and OGP standards.

On January 14, 2022, the first OGP Standards document was emailed out to you, Andrew, Darren, and Eduardo:



2022 New Club IT Standards

Ryan Wagner
To ● Andrew Dinh; ● Marc Radik Fused; ● Darren Kontaku; ● Eduardo Garcia

Fri 1/14/2022 10:22 AM

2022 New Club IT Standards.docx
19 KB

Happy Friday!

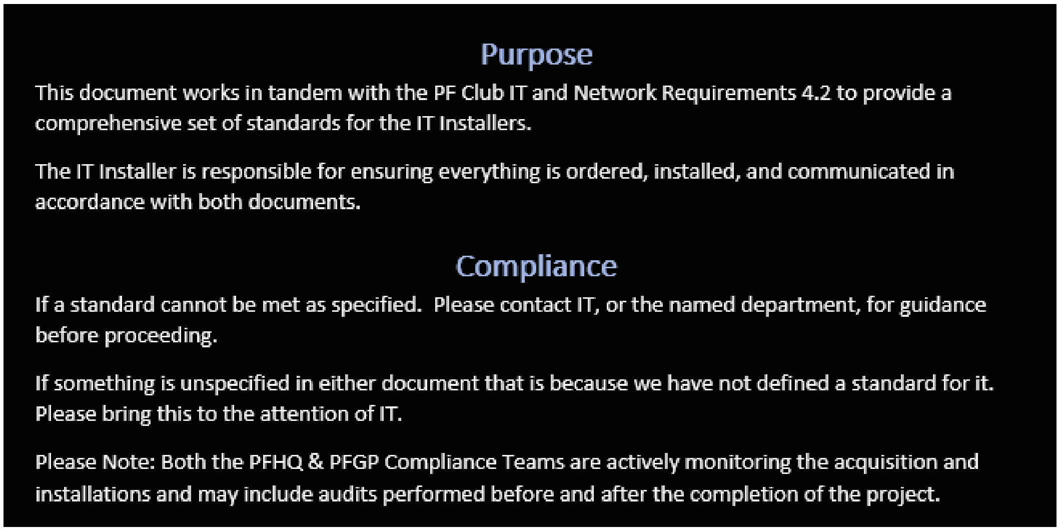
@Andrew Dinh @Marc Radik Fused This year, we are changing the current IT Standards. We will be upgrading older clubs to meet these new standards over the next three years and want to ensure that new clubs meet or exceed these standards. Attached is a word document that outlines the new standards. Please review and let me know if you have any questions.

NOTE: This document is primarily for you two. Please let me know if you are doing anything else that is not documented here. Long term, I want to have a complete SOP style document that will ensure we don't have to go back into a club after it's built to implement or change anything and ensure that we have documented everything that goes into a new club.

@Darren Kontaku @Eduardo Garcia Please review the document and let me know your thoughts as well. Your objective is to ensure that you have everything needed to fully support these clubs and have all the information in advance.

You responded to this email, and through both email and phone calls, we discussed this document in length. The list of stakeholders grew, the document became more details, and each update included you in the email recipient list. However, PFHQ and OGP continued to experience compliance issues; by April 2021, Josh and Bill were tired of failing compliance and getting emails from PFHQ. Eventually, resulting in Development turning over you and Andrew for me to manage. This resulted in the following being added to the standards document:

Exhibit 10B



Purpose

This document works in tandem with the PF Club IT and Network Requirements 4.2 to provide a comprehensive set of standards for the IT Installers.

The IT Installer is responsible for ensuring everything is ordered, installed, and communicated in accordance with both documents.

Compliance

If a standard cannot be met as specified. Please contact IT, or the named department, for guidance before proceeding.

If something is unspecified in either document that is because we have not defined a standard for it. Please bring this to the attention of IT.

Please Note: Both the PFHQ & PFGP Compliance Teams are actively monitoring the acquisition and installations and may include audits performed before and after the completion of the project.

It also marks the point where I began proactively communicating specific needs to ensure the bare minimum was met, trying to prevent compliance letters and assessment failures in advance. However, Maryville and Parkland were missing deadlines and letters showed up. On October 21, 2022, Andrew Dinh and I had the first of several conversations. Andrew took over as the only IT Installer for all New Clubs, Remodels, and Re-Equips for OGP, and I agree that he could utilize you in Maryland with the understanding that he was responsible for your work and results. As 2022 rounded out, Rockville became the worst IT Installer project of the year, with financial, compliance, and assessment failures found.

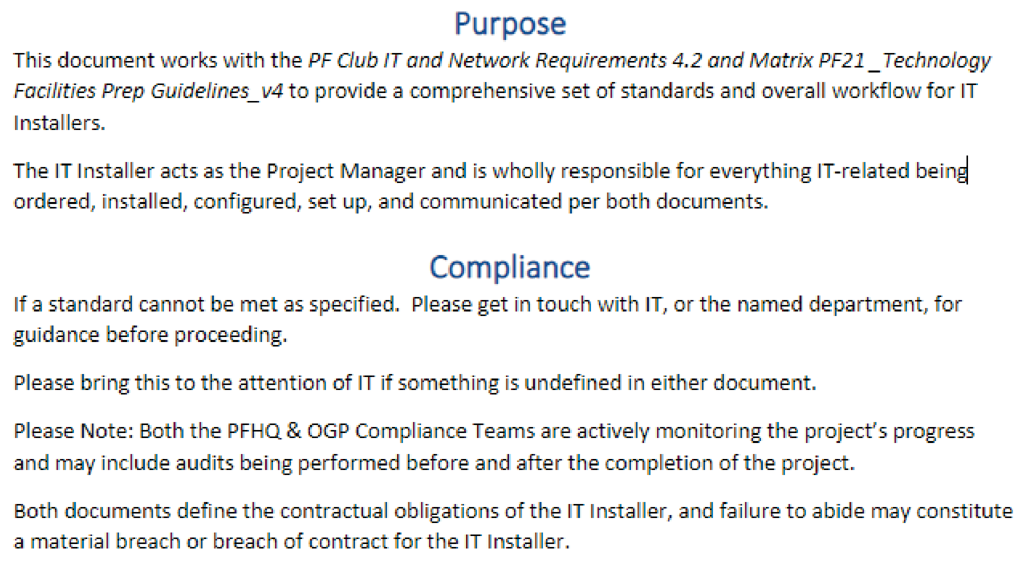
Rockville resulted in new safeguards and auditing. Those resulted in Reisterstown being found operating outside of PCI compliance and revealed that this had been an ongoing occurrence. There is never an acceptable situation where a club is open to the public, and PCI compliance is not in effect. This leads to more safeguards, audits, site visits, and other processes put in place. During the last few weeks, in conjunction with another project and inclusive of the increased measures put in place, we discovered that the wifi network you manage does not provide two essential wifi networks. When I asked you how long it would take you to implement the PCI-Compliant POS iPad and the Secure Vendor networks, you told me a month and tried to convince me that it wasn't necessary because we are replacing the wifi network.

Everyone must review the v3.8 zipped attachment and speak with me at our next meeting on Tuesday if you have any questions.

Moving forward - All correct processes, scopes of work, standards, and expectations must be met without exception.

Please take note of what the current OGP IT Standards v3.8 starts with:

Exhibit 10B



Purpose

This document works with the *PF Club IT and Network Requirements 4.2 and Matrix PF21 _ Technology Facilities Prep Guidelines_v4* to provide a comprehensive set of standards and overall workflow for IT Installers.

The IT Installer acts as the Project Manager and is wholly responsible for everything IT-related being ordered, installed, configured, set up, and communicated per both documents.

Compliance

If a standard cannot be met as specified. Please get in touch with IT, or the named department, for guidance before proceeding.

Please bring this to the attention of IT if something is undefined in either document.

Please Note: Both the PFHQ & OGP Compliance Teams are actively monitoring the project's progress and may include audits being performed before and after the completion of the project.

Both documents define the contractual obligations of the IT Installer, and failure to abide may constitute a material breach or breach of contract for the IT Installer.

From: Marc Radik mjradik@fusedtech.com
Sent: Wednesday, July 12, 2023 9:05 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>; Logan Ford <lford@osisupport.com>; Colin Lucena <clucena@osisupport.com>
Subject: RE: 12 July 2023 - Notes

CAUTION: This email originated from outside the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Reisterstown does not have a PE@PF TV. And I'm 99% sure they did not have a PE@PF TV before the remodel. I was not involved with the original Rockbot install, so I do not know what they did with that rockbot device. I know with Gaithersburg and Germantown remodel, they do not have a PE@PF TV either.

To my knowledge T-Max is neither Wifi or Ethernet. It is its own controller, talking to the other T-Max devices with its own wireless communication. Unless something has changed recently, TMax has never been a part of any network.

Marc J. Radik
Fused Technology Inc.,
(410) 670-7200 x101

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Wednesday, July 12, 2023 8:20 PM
To: Marc Radik <mjradik@fusedtech.com>; Logan Ford <lford@osisupport.com>; Colin Lucena <clucena@osisupport.com>
Subject: RE: 12 July 2023 - Notes

@Marc Radik

On Assets – yes and no. Get what you can. With the rack pulled out and redone – it was the opportune moment to complete the verification process. There was also a ton of things moved around and reinstalled, and part of the project onboarding step is to verify and correct things that were moved, adjusted, installed, etc. In this case – everything.

Rockbot – 5/2 is the standard, and most of our clubs do have 5/2. We allow 4/2 on some clubs, but Reisterstown has 5. The one assigned to PE@PF is currently not online.

Exhibit 10B

On T-Max – If this is an ethernet connection, work with the SOC to ensure it is connected to the correct network. If this is a WiFi connected for T-Max then it has to go on a more secure network and will require my involvement as we are adjusting some things to ensure things are put on the correct networks. At this time, the SSID and password used for radiance based wifi communications as restricted to cerdant and myself.

On Cameras – Once we have an approved layout for cameras, we can discuss what is reasonable to obtain for verification. If a cameras wasn't adjusted, moved, installed, etc then probabaly safe to say we don't need to include it.

On Punchlist – Starting yesterday, the punchlist deadline begins which is 10 August 2023. This is the collection and completion of all punchlist items. However, that is subject to two key factors – nothing on the punchlist can bring us out of PCI compliance or cause us to fail the PFHQ audit that is about to come.

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Marc Radik <mjradik@fusedtech.com>
Sent: Wednesday, July 12, 2023 7:31 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>; Logan Ford <lford@osisupport.com>; Colin Lucena <clucena@osisupport.com>
Subject: RE: 12 July 2023 - Notes

CAUTION: This email originated from outside the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

I'll get as much information as I can. I might not be able to get pictures of everything (i.e. AP's that are already mounted up high, etc…) but I'll get the serial numbers from cerdant. I'll do what I can to get serial numbers for the items I cannot get pictures of. Wasn't all this supposed to be gotten already from Cielo when they did the upgrades a year or so ago? FYI, I believe there are only 4 rockbot players for newer clubs and remodels. Main Club, Spa, Front desk, and 360. We stopped doing the PE@PF TV a little bit ago it seems.

I'm going back on Friday to complete a punch list of items, like the T-Max. They were unable to locate it while I was there today. Also, I believe the Locker Room TV's and DVR TV needs to be mounted. I asked Brandon to create a punch list for me. I will complete this punch list, and get these serial numbers on Friday. I will not be able to get any EEN camera info, as I don't have access, but they should easily be obtainable from EEN portal.

Marc J. Radik
Fused Technology Inc.,
(410) 670-7200 x101

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Wednesday, July 12, 2023 7:17 PM
To: Marc Radik <mjradik@fusedtech.com>; Logan Ford <lford@osisupport.com>; Colin Lucena <clucena@osisupport.com>
Subject: 12 July 2023 - Notes

Exhibit 10B

@Marc Radik Reminder of our conversation, I need a picture of all the IT equipment serial information at Reisterstown in an email to ITO@ohanagp.com.

From memory, we identified the following:

- Firewall
- POS Switch
- Ubiquity Switch
- WiFi Switch
- 4 Aps
- Wattbox PDU
- Wattbox UPS
- Crown Amp (x2)
- ZV module
- 5 Rockbot Players
- iPads (should be x3)
- Laptop
- 2 Non-POS Desktops
- Cradlepoint
- EEN Bridge
- EEN Switch
- EEN Cameras

You can ignore the SES PC, POS PCs, TVs, and MYEs.

If there is anything else we missed – we need that too.

A picture of the device information – minimally showing the Serial Number – is enough for us to get it done for Reisterstown.

@Colin Lucena @Logan Ford Next Step – I need a camera layout to review and approve so that the EEN cameras correctly cover the updated floor plan.

I want to finish this like yesterday; this should have already been completed.

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

Exhibit 10F

From:	Ryan Wagner
To:	Glenn Norris; Justin Drummond
Subject:	Reisterstown Debrief
Start:	Tuesday, July 11, 2023 11:30:00 AM
End:	Tuesday, July 11, 2023 12:00:00 PM
Location:	Microsoft Teams Meeting
Attachments:	image002.png image003.png

Sorry for the late response. This one fell through the cracks in the mix of the other emails.

Does 11:30 AM EST work?

Microsoft Teams meeting

Join on your computer, mobile app or room device

Click here to join the meeting <https://teams.microsoft.com/l/meetup-join/19%3ameeting_MjczMDMxZWItZGYzOC00MmY0LTg5Y2QtMDM4ZWZhY2M5NTcw%40thread.v2/0?context=%7b%22Tid%22%3a%2212be282d-af65-44c5-9b03-ca46dc2f46ee%22%2c%22Oid%22%3a%2241aaa976-a65c-4d39-9b99-476c29593ca1%22%7d>

Meeting ID: 216 499 682 957
Passcode: SsDoSc

Download Teams <https://www.microsoft.com/en-us/microsoft-teams/download-app> | Join on the web <https://www.microsoft.com/microsoft-teams/join-a-meeting>

Or call in (audio only)

+1 469-214-8508,,476413323# <tel:+14692148508,,476413323#> United States, Dallas

Phone Conference ID: 476 413 323#

Find a local number <https://dialin.teams.microsoft.com/d44639be-1769-4cd6-be1f-ae31789b582d?id=476413323> | Reset PIN <https://dialin.teams.microsoft.com/usp/pstnconferencing>

Learn More <https://aka.ms/JoinTeamsMeeting> | Meeting options <https://teams.microsoft.com/meetingOptions/?organizerId=41aaa976-a65c-4d39-9b99-476c29593ca1&tenantId=12be282d-af65-44c5-9b03-ca46dc2f46ee&threadId=19_meeting_MjczMDMxZWItZGYzOC00MmY0LTg5Y2QtMDM4ZWZhY2M5NTcw@thread.v2&messageId=0&language=en-US>

From: Glenn Norris <glenn@ohanagp.com <mailto:glenn@ohanagp.com> >
Sent: Monday, July 10, 2023 4:17 PM
To: Justin Drummond <Justin.Drummond@ohanagp.com <mailto:Justin.Drummond@ohanagp.com> >; Ryan Wagner <Ryan.Wagner@ohanagp.com <mailto:Ryan.Wagner@ohanagp.com> >
Subject: RE: Reisterstown Debrief

Yes, how about tomorrow or Wednesday around 11 either day.

Glenn Norris

Chief Financial Officer
Ohana Growth Partners, LLC

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd

Exhibit 10F

Timonium, MD 21093

www.planetfitness.com <http://www.planetfitness.com/>

“Culture eats strategy for breakfast”

From: Justin Drummond <Justin.Drummond@ohanagp.com <mailto:Justin.Drummond@ohanagp.com> >
Sent: Monday, July 10, 2023 3:20 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com <mailto:Ryan.Wagner@ohanagp.com> >; Glenn Norris <glenn@ohanagp.com <mailto:glenn@ohanagp.com> >
Subject: RE: Reisterstown Debrief

Thanks for the note.

Are all of us, including JB, syncing up one day soon to chat about build expectations?

Thank you.

Justin Drummond

Chief Operating Officer
Ohana Growth Partners, LLC

office 410-252-8058 x214
212 W. Padonia Rd
Timonium, MD 21093

www.planetfitness.com <http://www.planetfitness.com/>

“Culture eats strategy for breakfast”

From: Ryan Wagner <Ryan.Wagner@ohanagp.com <mailto:Ryan.Wagner@ohanagp.com> >
Sent: Friday, July 7, 2023 6:36 PM
To: Glenn Norris <glenn@ohanagp.com <mailto:glenn@ohanagp.com> >; Justin Drummond <Justin.Drummond@ohanagp.com <mailto:Justin.Drummond@ohanagp.com> >
Subject: Reisterstown Debrief

To state the obvious

* Development is responsible for building our product, which is our clubs.
* Building a club requires a waterfall project management methodology, which means the project goes from start to finish as planned without modifications.
* Ensuring the project is completed as planned, on time, and budget is critical to our success.
* The above is equally valid for remodels and re-equips.

Until recently, I thought the following was also equally obvious:

* PCI compliance - If billing data/transactions are involved, they must adhere to PCI compliance requirements.
* Fire Alarm Functionality – If we are open to the public, we should take appropriate action to ensure the system works properly.

Reason for today’s Visit:

* Merlowe was there in response to the Fire Alarm System going off “non-stop.”
* I was there to follow up on a problem brought to my attention by SES and our SOC about the SES/HVAC system.
* We agreed to go together so that I could share my insights on connectivity and she could share her insights on HVAC.

Penalties/Risks for not adhering to PCI Compliance include:

* Fines and Penalties
* Increased Audit and Assessments
* Damage to the PF Brand
* Suspension/Termination of Processing Privileges

2 of 3

Exhibit 10F

* Lawsuits and Other Legal Consequences

I have already confirmed that we were operating outside of PCI compliance. The time and materials it took Marc to bring us back into PCI compliance appear to have been less than an hour of labor and less than 20$ of materials. He may say the material cost was more, but I will point out that part of his work put our PCI compliance in a risky state, and during the post-work follow-up, we removed that risk. Thus reducing the total material cost.

Penalties/Risks for Operating without a Functioning Alarm System:

(Unlike PCI Compliance – I am not an expert on Fire Alarm Systems and rely on publicly available information.)

* Injury or Death
* Fines, Penalties, and Closure of the Business

 * It seems pretty consistent that most jurisdictions state that operating a business without a functioning fire alarm system is illegal, particularly with open to the public.

* Lawsuits and Other Liabilities
* Voided Insurance Policies or Refusal to Cover Related Damages
* Damage to the PF Brand

Merlowe told me that the system has been alerting and notifying her “non-stop” for quite a while. Merlowe and I Reviewed the Fire Alarm System logs, which showed alternating NAC 1 and NAC 2 fault codes at a frequency that matches her description of “non-stop.” Googling that code, I can see that the NAC is Notification Application Circuit, and the many diagnostic guides indicate that this comes from a cut, broken, damaged, or loose wire connecting the annunciator to the horns, bells, speakers, strobe lights, etc. This part of the system would notify people of a problem and save lives. Merlowe said the annunciator is a new part of the system installed in this remodel. The fault error alone is not enough to determine if the system would or would not function properly. However, all reference points state that a qualified fire alarm technician should address the NAC fault as quickly as possible to ensure the safety of all building occupants.

One thing that stood out to me, is that the Fire Alarm System faults were constant for days – or longer. We stopped scrolling through the logs after a couple days of it being the exact same faults repeatedly. Per the logs, the faults stopped right before I arrived. Merlowe only walked into the club a little bit before I did, and neither of us told anyone to do anything. I never said anything about why I was there, and I believe Merlowe only said she was there to check on the Fire Alarm System. How did they know what the issue was, and how did they “fix” it so quickly? If it was such an easy and quick fix, why did they let it go on for so long and were we at risk the entire time?

Ryan Wagner

Vice President of IT
Ohana Growth Partners, LLC

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093

www.planetfitness.com <http://www.planetfitness.com/>

“Culture eats strategy for breakfast”

3 of 3

Exhibit 10K

From:	Ryan Wagner
To:	Glenn Norris
Subject:	RE: Recap from meeting with Josh Beyer this morning
ate:	Friday, September 1, 2023 5:02:47 PM
Attachments:	image001.png ohanagrowthpartnersfinallogo_7fa8dba2-2909-40ee-839a-12ba06da3de6.png v4.0.zip

Yes, sorry for the gap - it has been go-go-go non-stop all day.

The meeting is at 8:30 am

The established plan:

- We meet every Friday morning. Just the two of us for the first month to sync and align. Then bring in who we need to for further progress.

Josh Ask:

- How does he know things are being done and on time.
    - We reviewed the existing checklist and he said that was great and exactly what he needed. He acknowledged that he has never seen Andrew present this at any meeting and he is committed to making sure he has an updated checklist from Andrew by Monday morning.
    - I followed up with that to provide him an updated checklist that broke out items better and enhanced the when column with context to help everyone understand what and when.

I highlighted a few key parts of the document that address issues that need to be addressed before we have an approved floor plan and critical issues that might seem innocuous may have significant risks for us by not doing it.

- We don't use this or that type of cable because… they can cause fires or release toxic gas
- We need the server room to be within a specified distance to drop points like the server room because… the cable can't transmit further and it causes network issues.
- We need to use grommets at certain times because… it will keep the cable from being damaged and require replacement and can prevent other risks
- We need to be mindful of how close low-volt cables are to electrical conduits because… the electrical conduits can cause network/internet issues

We discussed key times when PFHQ requires things to be done:

- Ordering of required hardware
- Compliance Forms
- Physical Pre-Sales Sites required geotagged photos submitted when OSI or other non PFHQ certified vendors do the work
- Pre-Open certification when OST or other non PFHQ certified vendors are doing the installation

We discussed how the first two take less than 5 minutes of combined effort and how in my opinion if that isn't being done, and HQ is getting on us about it, then we shouldn't assume the harder stuff is

Exhibit 10K

being done. He agreed.

He said that he understands that this was only an extremely small portion of the issues and we will need the time to go through it in small bite size chunks. We will be walking Takoma Park as it approaches the open date and we will go through the 15 page document item by item so he can see how little is done to meet requirements and standards. Even the little part we did cover, he appeared to understand this really is the tip of the iceberg and he understands those whys better now.

He said that Bill and the rest don't need to understand the why, only that we are doing it. I didn't take that as a hiding thing from them, but rather a "no bill – you can't decide what is important. It must be done even if you don't understand it or the why".

He wanted to push for Andrew to do 100% including adding assets into Woven. I said that I would prefer to have the Help Desk onboard the equipment for two reasons. One I know it will be done correctly, and I also know that it's very time consuming for anyone to learn how to do it right. The example I gave is "you can't put ZV for the name of the ZeeVee Modulator – you have to put in ZeeVee or else we end up having to redo it later anyway" I said that if Andrew can get the checklist done every week and is meeting the standards which includes a much easier task of taking picture of the equipment plate that has a serial number then I have no problem talking about it being added at a later time. He agreed.

Final thing, Since the checklist was updated. I replaced the old standards document to use the reference document that you saw because It is much easier for someone to see in black what PFHQ says and then in red how we have chosen to meet that. It has all the necessary information for Andrew and everyone that has looked at it, which includes a few people who are part of the team that writes the PFHQ standards document, says that it's amazing and have asked for a copy to use and show others.

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Friday, September 1, 2023 4:09 PM

Exhibit 10K

To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Subject: Recap from meeting with Josh Beyer this morning

Ryan, do you have a recap to share with me from your meeting with Josh Beyer this morning?

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Thursday, August 31, 2023 4:01 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Glenn Norris <glenn@ohanagp.com>
Subject: FW: meeting at 2PM tomorrow- agenda items to discuss

Good meeting, thank you. See some notes below in red to make sure you follow up on with me.

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Wednesday, August 30, 2023 3:37 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Glenn Norris <glenn@ohanagp.com>

Exhibit 10K

Subject: meeting at 2PM tomorrow- agenda items to discuss

Ryan, this is our agenda tomorrow.

1. Goals for September-discuss and make sure we agree on the execution timing
    a. Fire and Hire – send me the job description & KPI-send me the updated JD and KPI by 9-15.
    b. Access for all users is one log on only per person, ease to log on and easier access to a consistent cloud files format. Communicate and Trial it before a blanket install
    c. Meet with Josh Beyer(one on one) each week for 30 minutes to an hour to align IT and Development. Send an email to me post meeting from both of you on the topics discussed and issues resolved. When is that meeting time and day-(Friday at 830) ? Tomorrow's meeting- goal is to be in total compliance when a project is deemed complete/open for business……..discuss who will be the doer's and accountable parties ………the accountable parties must work as one to make sure the doer's see a unified front. Being in every meeting for IT is critical from planning to finish. Build Trust in each other- no non-verbals or verbals that belittle others during meetings to recap project status and in a Green, Yellow or Red mode.
2. IT Budget to Actual through July 31, 2023 for each company. Next Tuesday at 1PM
3. Cielo update on what they still have in our cash……….show me the projects they will work on to get it to Zero by 12-31 or how they will still owe a balance and pay us that balance that is anticipated by 9-30-23. Need update on status by Monday.
4. Comcast Double billing update. Is it resolved? If not, why? Need a plan to get all $$ returned by 9-30-23. Need update on status by Monday.
5. Using Monday.com in the interim for Development/IT projects…………hire someone that can manage this and attend development meetings. Refer to 1c.
6. Discuss the replacement of Andrew Dinh with Josh Beyer – what must Andrew do by 9-30-23 to prevent this replacement from occurring.
7. Timeline of IT changes and potential budget for those changes to occur- month by month time line through 12-31-24. Must do this with Glenn ahead of any implementation . Need 30 days in advance of any launch.
8. KPI Form- let's review for changes. KPI for August is Sept 14. Let's review for updates.
9. What is your biggest challenge each day? Tell me ???
10. What can I do to help you? Tell me???

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

Exhibit 10K

5 of 5

Exhibit 22F-1

How Standards Help You

Many conversations have occurred around the word “standards” and caused us to lose focus on the why until it became an immediate issue that directly impacted us. This has resulted in electrical damage, poor performance, slower resolutions, increased downtime, higher costs, member complaints, lower listen360 scores, lost revenue, additional burdens on team members, more projects to fix, and a rack falling off the wall. We have blamed the current problematic symptom and allowed the standards to be disregarded because the conversation never moved past words on a page. This is the first step many have taken to correct this because this impacts all of us equally.

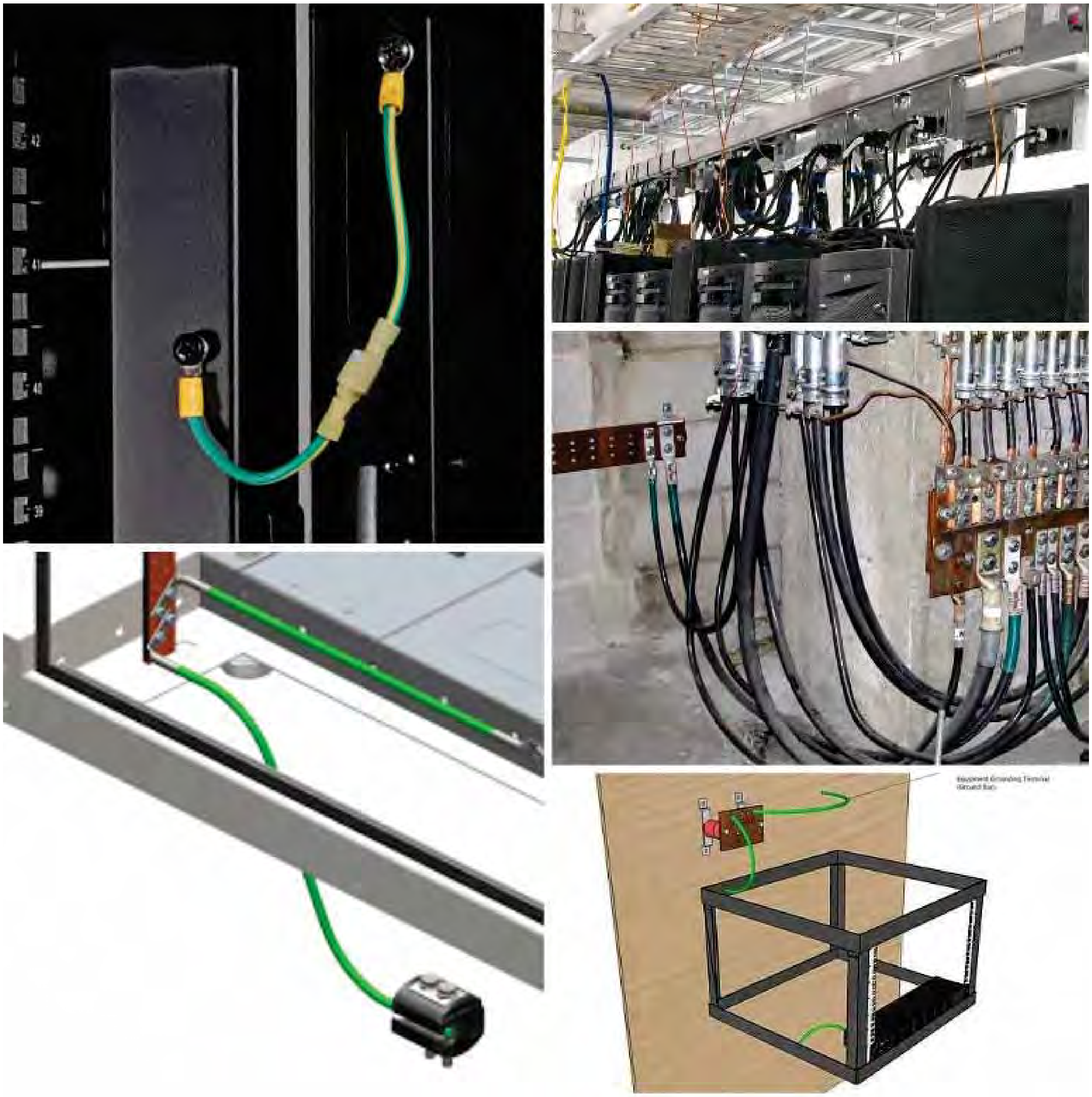
Electrical Standards

Electrical racks must be adequately grounded to prevent fires, injuries, and equipment damage. Adequate grounding involves two key components:

- A connection from the rack to a reliable ground outside the rack. Ground fault circuit interrupters, which significantly reduce electrocution risks, exemplify the importance of proper grounding. All our racks will be upgraded to meet safety standards by the end of 2024 to address these safety concerns.
- A grounding cable inside the rack frame attached to the door ensures safety during electrical surges by preventing electrical arcs between the door and frame. This cable directs any surge back to the ground connection, protecting anyone interacting with the rack.

Here are some examples of how this is accomplished:

Exhibit 22F-1



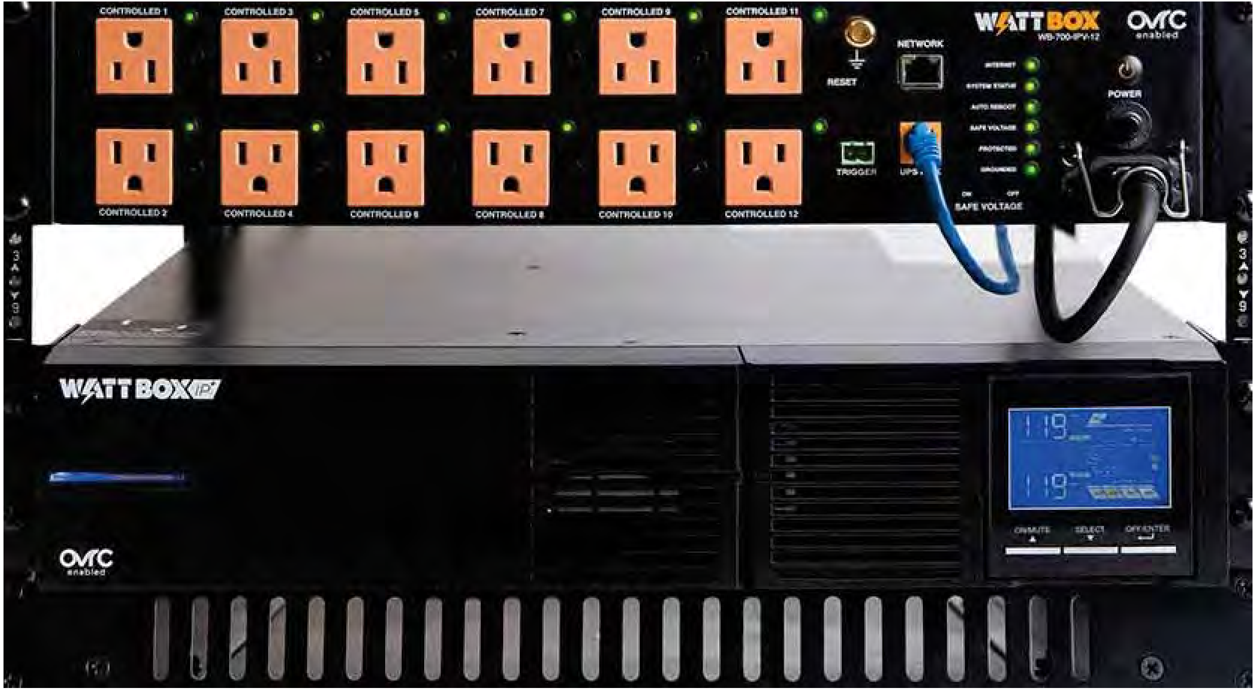
Power Conditioners

You may only know these devices as power strips and universal power supplies (UPS). Still, the equipment we use is far more advanced and not only prevents surges and conditions the electrical current to be the correct voltage, amplitude, and frequency by performing power factor correction, noise suppression, transient impulse protection, nonzero low and high-frequency impedance, and more.

We cannot add to or augment these systems with another power supply, UPS, power strip, etc.

Exhibit 22F-1

- Wattbox plugs face toward the front, not toward the rack's inside. This allows you to see the status lights and the plugs themselves.
- The network cable is how we remotely manage the device.
- The power button and reset switch are easily accessible in case an IT support team member needs you to restart that device.
- Both devices are necessary for proper function and are purchased as a kit. They are sold separately in case one of the devices is damaged, such as from overloading, improperly racked, or improperly connected.



Remote Power Management

Wattbox also enables remote power management but requires the equipment to be connected to its assigned location. Otherwise, we will not use it to resolve or troubleshoot issues because doing so could create new problems.

Separated Electrical Circuits

Electrical issues can disable an entire IT rack until an electrician resolves it. Using an extension cord might appear as a quick solution, but this approach can lead to several hazards, including:

- Overloading the cable or circuit could result in fire or equipment damage.
- Physical damage to the cord from foot traffic, carts, or doors compressing it.
- Potential hazards from using indoor cables in moist environments such as clubs.

To prevent these risks, we install a second quadplex on a separate electrical circuit. If one quadplex fails, the system can temporarily switch to the other without added risks. A quadplex looks like a regular receptacle but functions differently.

Exhibit 22F-1

A rule of thumb is that you will see a metal box on the wall with four outlets for a quadplex, and any with two outlets or face-plated into the wall are receptacles.

Electrical Summary

Notify the Help Desk if one or more of these are true:

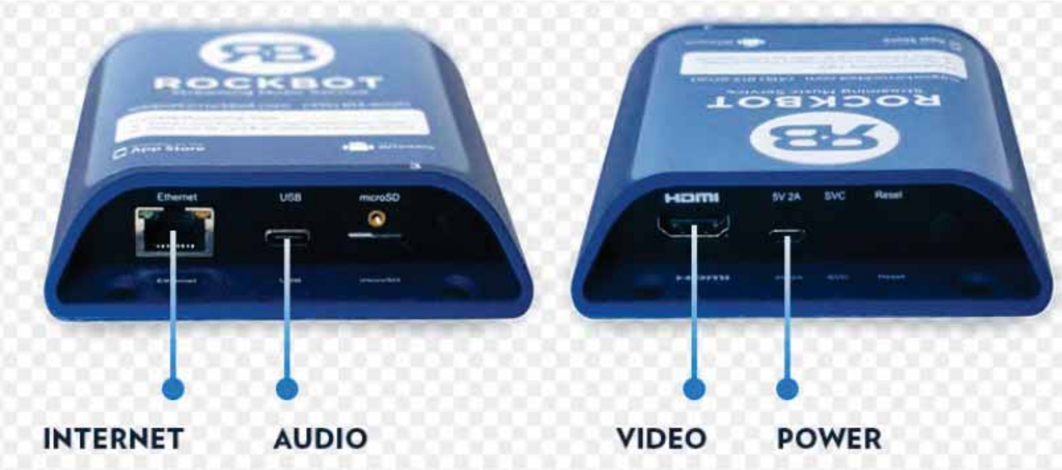
1. **The IT rack and door are not adequately grounded.**
2. **The IT Closet does not have two quadplexes reasonably accessible to the IT Rack equipment.**
3. **The Wattbox device with the outlets is not facing forward as shown.**
4. **You are missing one or both devices.**
5. **Both devices are not securely racked inside the rack, near or at the bottom, and the door can close and lock.**
6. **No ethernet cable with the outlets is connected to the Wattbox device.**
7. **The Wattbox device with the outlets is not connected as described here:**
   - Port 1: POS Switch
   - Port 2: Primary Internet Modem
   - Port 3: Backup Internet Cradlepoint: IBR900
   - Port 4: Back Office Switch
   - Port 5: Wi-Fi Switch
     - Juniper Firewall on Deeblue Wi-Fi Sites
   - Port 6: IT Utility PC
     - Ruckus Wi-Fi Switch on Deepblue Wi-Fi Sites
   - Port 7: SonicWALL Firewall
   - Port 8: Eagle Eye Bridge
   - Port 9: Eagle Eye Switch

Rockbot Standards

Ethernet Connection for Rockbot Players

The Rockbot Players tend to lose their wireless network connection, which requires a team member to remove the player from behind the TV, connect it to a PC, and manually reconnect it to the Wi-Fi. This problem goes away when they are connected via Ethernet.

Exhibit 22F-1



Side Mounted Rockbot Players

Access to the device is obscured and can become dangerous for team members to access when not mounted accessibly. This problem goes away when they are mounted to the sides of the TV, and the TV is still able to obscure their visibility to the Members.

Rockbot Summary

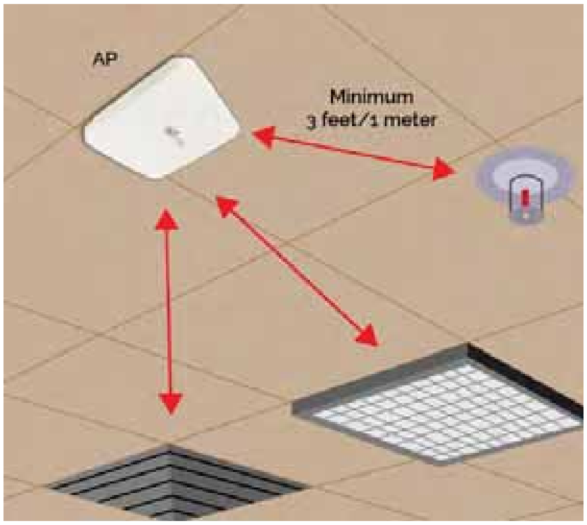
Notify the Help Desk if one or more of these are true:

1. **Rockbot players are not safely accessible.**
2. **Rockbot players are not connected with an ethernet cable.**

Wi-Fi Access Point (AP) Placement

Wi-Fi access points are mounted from the ceiling and typically on a pole, and you should know three things about their placement.

- For optimal signal operation, they should be 3 feet from lights, sprinklers, and vents, as shown in this diagram.



5 of 12

Exhibit 22F-1

- Not all access points transmit and receive signals the same way. How and where they are mounted can change the signal quality and coverage area.
- Almost every club will have four APs; the rest have five.

Wi-Fi Summary

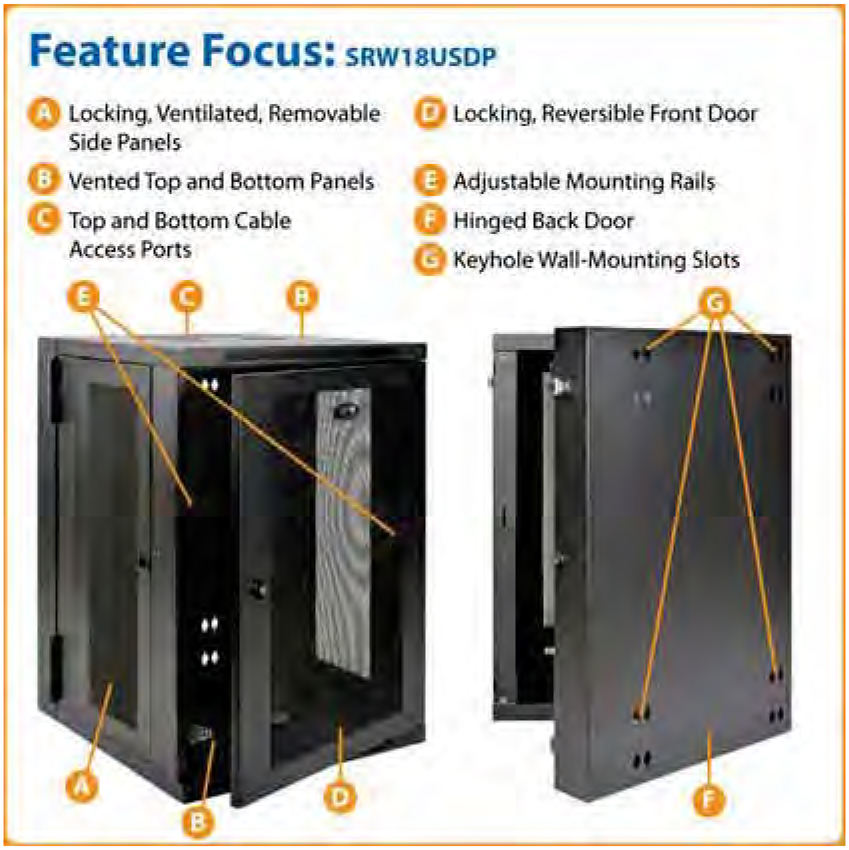
Notify the Help Desk if one or more of these are true:

1. **After a remodel or Wi-Fi upgrade, all your APs are in the exact location.**
2. **APs are within 3 feet of a sprinkler, ceiling light, or air duct.**

Rack Standards

Lockable Enclosure

The Triplite SRW18USDP was selected to optimize space, support the weight of the assigned equipment, meet PCI requirements, and provide easy access to the equipment's front, back, and sides.


Feature Focus: SRW18USDP
A Locking, Ventilated, Removable Side Panels
B Vented Top and Bottom Panels
C Top and Bottom Cable Access Ports
D Locking, Reversible Front Door
E Adjustable Mounting Rails
F Hinged Back Door
G Keyhole Wall-Mounting Slots
E
C
B
G
A
B
D
F

The rear side of the equipment is accessible because of the hinged back door. To avoid injury and damage to the equipment:

- The correct rack model must be used.
- The rack is securely mounted to the backing board.
- The equipment in the rack is correctly racked.

Exhibit 22F-1

- Nothing is on top of the rack.
- Nothing is obstructing the rack from opening properly.
- Cables going into the rack have enough slack to ensure the door can be fully opened with just a tiny bit of slack left over.

Securely Racked Equipment

All equipment is racked inside the rack with nuts and bolts that secure the equipment and prevent it from moving without removing those nuts and bolts. Smaller items are placed on dedicated shelves or mounted drawers. For safety, efficiency, and the longevity of the equipment:

- o This keeps things organized and helps prevent items from falling out or onto each other.
- o Prevents stacked items from blocking airflow and transferring heat to/from each other, which could cause them to overheat and malfunction.

Exhibit 22F-1

Secured to Backing Board

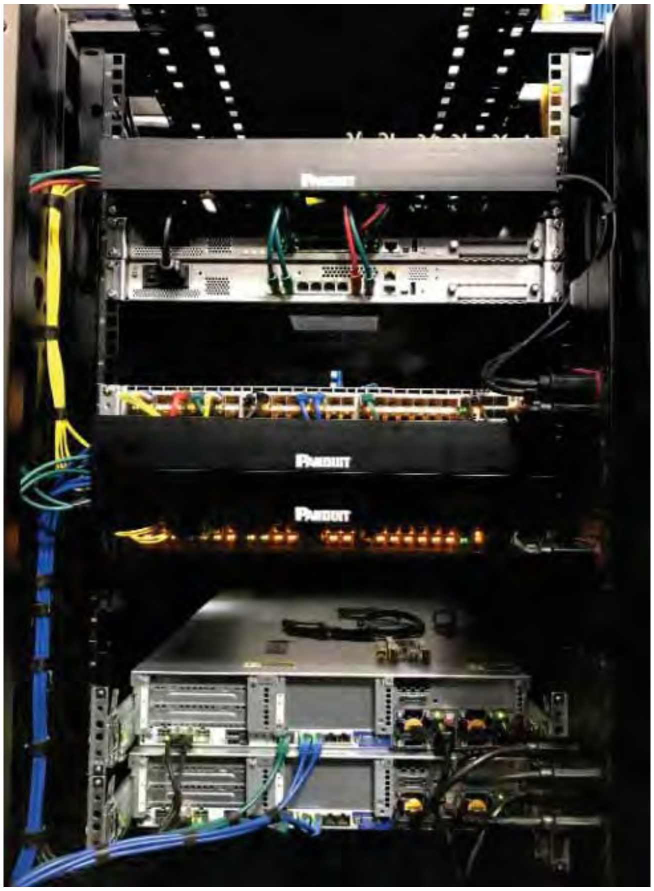
When the rack is mounted correctly to the wood backing board, it will support 250 lbs. Only defined equipment is intended to be placed inside the rack with nothing on the rack to ensure the safety of our team members and the equipment.

- Wood backing board provides safety from humidity and temperature and acts as a secure flat mounting surface.
- THE SES PC is placed on a separate shelf mounted on the backing board and never inside the rack.
- A UPS is mounted on the backing board and provides power to the SES PC and other equipment not assigned to the Wattbox.
- The Cradlepoint modem is mounted higher than the rack on the backing board to ensure optimal signal quality.

Cable Management

Power and Network cables are run through separate cable management channels. Power cables interfere with the performance of network cables, which translates to a slower and less reliable network/internet. Cable management keeps them organized so you can safely access things and follow instructions without struggling with a tangled mess.

Exhibit 22F-1



Rack Summary

Notify the Help Desk if one or more of these are not true:

1. **Cabling and network equipment is at the top.**
2. **Heavy items like power supplies are at the bottom.**
3. **Everything inside the rack is racked or on a racked shelf.**
4. **Differently colored ethernet cables are used for different networks.**
5. **Cables are neatly bundled and use cable management.**
6. **SES PC is anywhere except on a shelf mounted to the wood backing board.**
7. **The Cradlepoint is anywhere except mounted higher than the rack to the backing board.**
8. **The IT Rack is not mounted to a wood backing board securely affixed to the wall.**
9. **The sides are securely in place, and the back and front are closed and lockable.**
10. **You have more than one rack.**

Cables

Purple Cables = POS Network

Cable Colors help you identify the wired PCI-compliant network connecting the POS machines. We are not in PCI compliance if:

Exhibit 22F-1

- Anything else is connected to a PCI-compliant network.
- POS machines are connected to any other network.
- Any device we own that is used to key in payment information is connected to a non-PCI-compliant network. This includes tablets used to sign up members when their payment information is typed in.

Only Logically/Cerdant and the head of IT can authorize a new connection or the move of a connection. The Help Desk, IT Vendors, and other IT team members work with them and are bound to the same restrictions.

If anyone else asks you to connect, disconnect, or move a connection, you must immediately contact Logically/Cerdant for approval and guidance. PFHQ says this includes ownership and everyone else.

Other Network Cable Colors

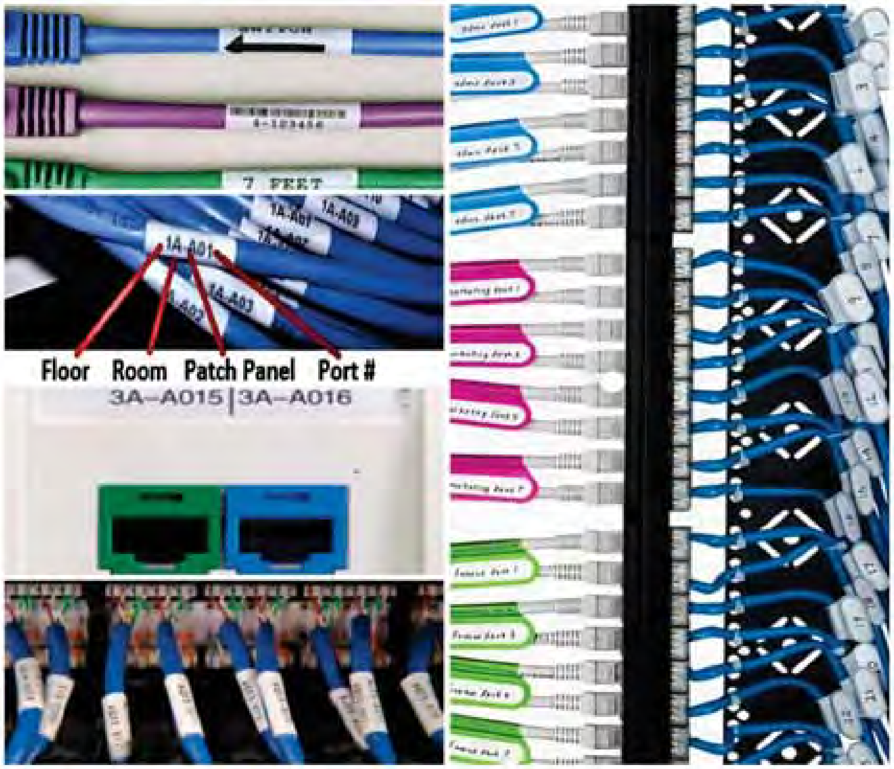
Other cable colors are used to identify the different networks. This is not limited to the IT closet/rack and applies to all cables used throughout the club. Cable runs visible to the members can be placed in cable channels that hide the wires and match wall/ceiling colors.

Color	Network	About
Purple	POS	**PCI Compliant Wired Network**
Yellow	Internet	Connect Modems to Firewall
Black	Back Office Network	Majority of Network Connections Staff and Equipment – No Guests
Green	Wi-Fi	Connect Access Points to the Rack and Wi-Fi equipment in the Rack Green Cables carry five different networks **Including the Wireless PCI Compliant Network**
Orange	VoIP	Voice over IP (VoIP) Our phone system that uses the internet
White	IT Network	Currently Not Deployed Reserved for IT Monitoring and Management

Exhibit 22F-1

End-to-End Labels

Labels help you quickly identify ethernet wall jacks, the connected network, the length of cables, where they came from, and where they go. Faceplates and wire ends should also be labeled.



Commercial Plenum (CMP) Rated (CMP)Cables

In the past, we may have used ethernet cables we now know could release toxic gas. To ensure everyone's safety, we have selected a commercial-grade cable that will not release poisonous gas and meet the National Fire Protection Association standards NFPA272 and 90A.

Not all jurisdictions have banned these cables, and passing a fire or building inspection may not ensure your safety. These cables will release the gas if there is a fire, but they can also release the gas without warning if the coating is exposed to enough heat, including ambient heat.

Commercially Approved Plenum Rated Cables:

- Ends with P like CMP, CATVP, CL3P, and CL2P

Plenum Rated Cables that are NOT rated for commercial use:

- Ends with an X like CMX, CATVX, CL3X, and CL2X.

Toxic cables still manufactured in the USA:

- Ends with an R, like CMR, or looks like one of those other examples without the X or P, like CM.

Cable Runs Less Than 328 Feet

When they exceed 328 feet, the signal might be too weak for a stable connection, which can cause dropped connections and reduced performance. 328 feet is the length of the run, including the cable length used as slack and continuous count through patch panels.

Exhibit 22F-1

Minimum Distance from Electromagnetic Interference (EMI)

When electrical sources and signal transmission cables are run together, the signal degrades too much, resulting in dropped connections and noticeably reduced performance. Running network cables one foot away instead of with or directly next to these electrical sources is all it takes to prevent this problem.

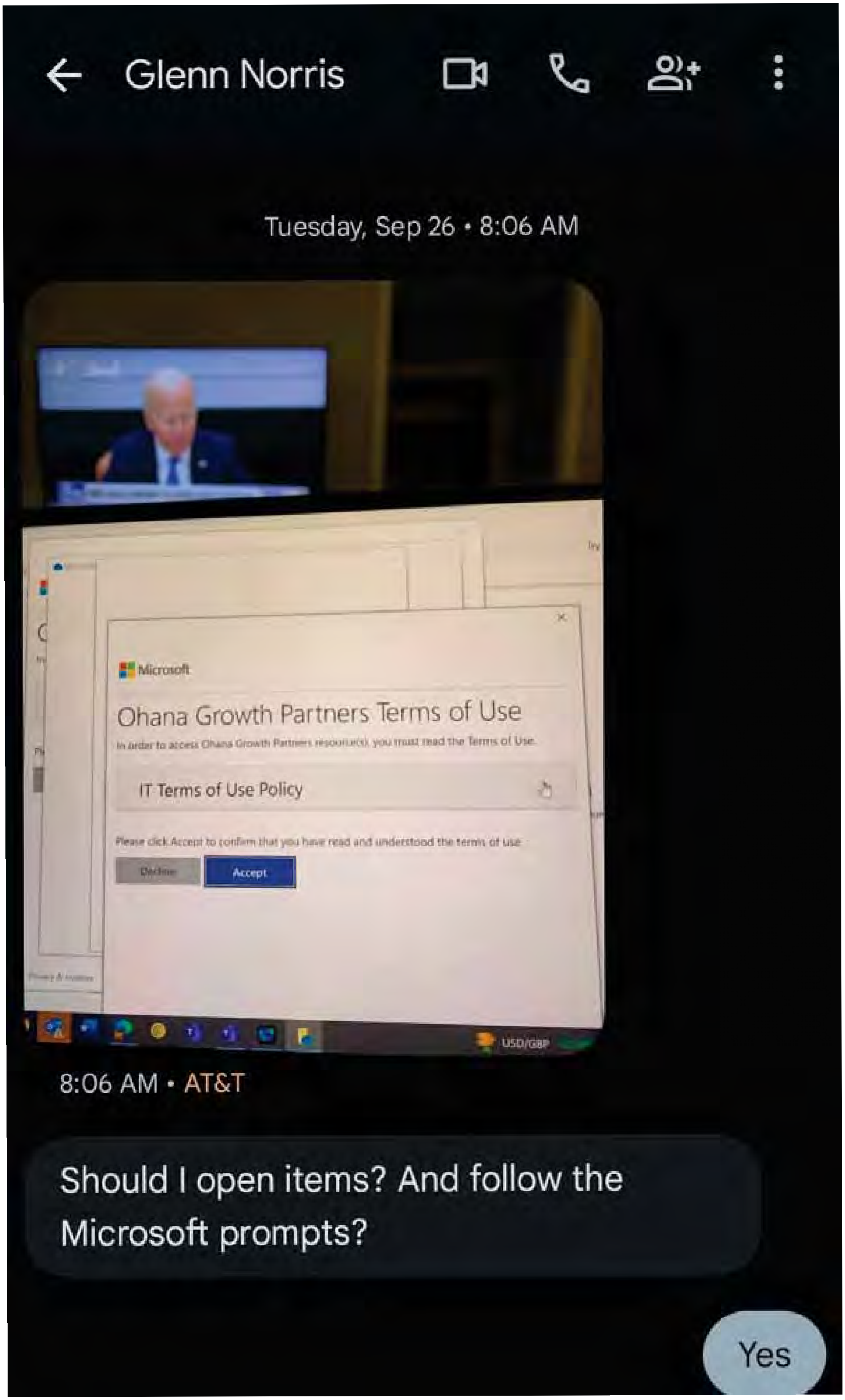
3 Common Signal Cables:

- Ethernet for Internet/Wi-Fi, Phones, and Security Cameras
- Coax for TV
- HDMI for Video

2 Common Electrical Sources

- Runs of Electrical Cables for outlets and other equipment
- Rows of Ceiling lights

Exhibit 2H-1



Glenn Norris

Tuesday, Sep 26 • 8:06 AM

Microsoft

Ohana Growth Partners Terms of Use

In order to access Ohana Growth Partners resource(s), you must read the Terms of Use.

IT Terms of Use Policy

Please click Accept to confirm that you have read and understood the terms of use

8:06 AM • AT&T

Should I open items? And follow the Microsoft prompts?

Yes

1 of 1

Exhibit 22H-2

IT Usage, Privacy, and Data Protection Policy

1. Scope

This policy applies to all users accessing our IT resources, including computer equipment, systems, network connections, third-party services, software, and programs used by the company, regardless of location or device.

2. Acceptable Use

Users must utilize IT resources for business purposes only. Prohibited activities include:

- Harassment, illegal activities, or any actions violating this policy.
- Unauthorized copying or distribution of copyrighted material, including peer-to-peer file sharing.
- Accessing, sharing, or distributing obscene or offensive content.

3. Security Measures

Users must:

- Use a VPN when accessing the network remotely.
- Regularly scan devices for malware and viruses.
- Keep all devices updated with the latest security patches.
- Avoid tampering with, modifying, or changing hardware, software, or systems without IT authorization.

4. Data Management

Users must:

- Save all data to approved cloud-based sources.
- Avoid using external storage devices unless explicitly approved by IT.
- Not save files locally or install unapproved programs or applications.

5. Third-Party Services

Users must be aware that data stored or transmitted through third-party platforms may be subject to their respective privacy policies and terms of use. Ensure that any third-party services used comply with company policies and data protection standards.

6. Data Collection

The company collects, stores, and uses a range of data for security and identification purposes, including:

- Biometric information such as voice prints, facial recognition data, and fingerprints.

Exhibit 22H-2

- Information about how, when, and where services are used, including user and device details. This data is used to improve our services and may be shared with third parties in compliance with applicable laws and regulations.

7. Reporting

Users must:

- Report any suspicious activity, unauthorized access, or policy violations to the IT department immediately.
- Follow established procedures for reporting security incidents, providing detailed information about the incident.

8. Compliance with PCI DSS

To ensure compliance with PCI DSS, users must adhere to the following additional requirements:

Customized Implementation:

- Tailor security controls to meet PCI DSS requirements while supporting operational needs and innovation.

Meeting New Requirements:

- Plan and implement new security measures, such as stricter access control and enhanced monitoring, by the required deadlines.

Continuous Compliance:

- Adopt continuous security monitoring and regular internal audits to maintain compliance.

Improved Reporting:

- Ensure meticulous documentation and record-keeping of all security measures for thorough ROC reporting.

9. Reporting Compliance Issues

Any compliance issues should be reported to the following authorized personnel:

Ohana Growth Partners Authorized Personnel:

- **Ryan Wagner**
  - Vice President of IT
  - Ohana Growth Partners, LLC
  - Office: 410-252-8058 x109
  - Address: 212 W. Padonia Rd, Timonium, MD 21093
  - Website: www.planetfitness.com

Exhibit 22H-2

PFHQ Escalation Contacts (for urgent situations):

- **Geoff VanMaastricht**
    - Security and Compliance Analyst
    - Planet Fitness World Headquarters
    - Address: 4 Liberty Lane West, Hampton, NH 03842
    - Phone: 603-319-6740

When PCI compliance issues are not resolved internally, they may be escalated to payment processors such as Visa and Mastercard. Non-compliance can result in significant penalties, fines, and restrictions on processing card payments. Prompt resolution of compliance issues is crucial.

- **Visa**: PCI Compliance | Keeping Customer Data Safe
- **Mastercard**: Site Data Protection (SDP) Program | PCI DSS Compliance

10. PCI DSS Information Sources

- **PCI Security Standards Council**: Protect Payment Data with Industry-driven Security Standards, Training, and Programs

Please review and adhere to these policies to maintain our security standards. For any queries or further clarification, contact the authorized personnel listed above. Thank you for your cooperation and commitment.

3 of 3

Exhibit 9C

OHANA GROWTH PARTNERS, LLC	**IN THE**
Plaintiff,	**CIRCUIT COURT**
vs.	**FOR**
RYAN DILLON-CAPPS	**BALTIMORE COUNTY**
Defendant.	**FILE NO.: C-03-CV-24-002264**

PETITION TO SHOW CAUSE AND FOR CONSTRUCTIVE CIVIL CONTEMPT

Plaintiff, Ohana Growth Partners, LLC. ("Plaintiff" or the "Ohana"), by its undersigned attorneys, and pursuant to Maryland Rule 15-206, hereby moves this Honorable Court to require Ryan Dillon-Capps ("Dillon-Capps" or "Defendant") (they/them) to appear before this Court and show cause why they should not be held in constructive civil contempt for knowingly violating this Court's Temporary Restraining Order entered June 17, 2024. In support of its Petition, Ohana states as follows:

1. At 12:18 p.m. on June 14, 2024, Ohana filed a Complaint alleging that Defendant breached their duties as Ohana's employee, specifically refusing to provide Global Administrator rights to Ohana's software systems and Internet domain name registrations to Ohana's officers and designees. Instead, Defendant eliminated all Global Administrator rights other than those they possessed.

2. Contemporaneously with the filing of the Complaint, Ohana filed a Motion for a Temporary Restraining Order ("TRO") requiring Defendant to (1) provide Global Administrative Rights for Ohana's Microsoft 365 Account to Phil Leadore of Hartman Executive Advisors and cease and desist the use of any of access to or use of Ohana's Microsoft 365 Account and related applications, including Ohana's email systems; and (2) Provide Administrative Rights for Ohana's GoDaddy Account to Phil Leadore of Hartman Executive

Exhibit 9C

Advisors and cease and desist of the use of any of access to or use of Ohana's GoDaddy Account and related Internet domain name registrations.

3. At 11:49 a.m. on June 14, 2024 Ohana's counsel transmitted copies of the subsequently filed Complaint, Motion for TRO and other papers to Defendant. The email advised of Ohana's intention to seek Court action on the Motion for TRO as soon as possible.

4. On June 17, 2024 at 10:50 a.m., the Court (De Simone, J.) granted the Motion for a TRO. A hearing on a Preliminary Injunction was set for June 26, 2024 at 9:00 a.m.

5. At 11:06 a.m. the TRO was docketed.

6. At 11:24 a.m., Defendant was personally served with hard copies of the Complaint, Summons, and Motion for TRO.

7. At 11:51 a.m., Ohana's counsel emailed Defendant with a copy of the TRO signed by the Court and docketed.

8. At 2:45 p.m., Ohana posted the $1 bond required to effectuate the TRO.

9. At 6:41 p.m., Defendant emailed Phil Leadore asking him to confirm that he was still interested in receiving administrative access, even though the TRO expressly directed them to provide Leadore access.

10. At 9:59 p.m., Defendant emailed Ohana's counsel requesting guidance for how they should comply with the TRO.

11. On June 18, 2024, at 8:39 a.m., Ohana's counsel forwarded the Court's Order setting the June 26, 2024 hearing for Preliminary Injunction and providing detailed directions on what Defendant must do to comply with the TRO, and further advising Defendant that their failure to comply by 12 P.M. will result in Ohana pursuing a finding of contempt.

Exhibit 9C

12. At 1:12 p.m. Plaintiff's counsel emailed Defendant that, in light of their non-compliance, Ohana is proceeding with efforts to hold Defendant in contempt.

13. At 1:26 p.m., Defendant emailed Ohana's counsel asserting that the TRO asks them take "illegal action."

14. Specifically, they allege that the TRO contemplates a violation of the "PCI Data Security Standard" ("PCI DSS"). PCI DSS was developed to encourage and enhance payment account data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data. However, PCI is not a federal, state, or local law. See https://www.pcisecuritystandards.org/about_us/. The PCI DSS is maintained by the Payment card Industry Security Standards Council, an independent entity established by the major card brands in 2006. The U.S. government is not involved, is not responsible, nor maintains enforcement mechanism associated with PCI. Rather, this is payment card industry self-regulation that is enforced via **contracted** services between merchants and acquiring banks and processors. Failure to meet PCI obligations imposes contract-based penalties that can include fines, penalties, and suspension or termination of payment card processing services. Thus, the PCI DSS provides no legal basis for Defendant's refusal to comply with the TRO.

15. Notably, Defendant does not dispute that:

a. On May 20, 2024, without authorization from Norris or other senior executives, Defendant severed and discontinued all administrative access to the Ohana MS 365 Account that had been held by other Ohana employees, as well as the Global Admin rights provided to Ryan Brooks, Ohana's contractor;

Exhibit 9C

b. Ohana management immediately and strongly objected to Defendant's unilateral action, and starting the next day, May 21, 2024, and in at least six subsequent separate written directives from May 21 to May 29, 2024, management ordered Defendant to instate Ohana officers and Brooks with administrative rights for Ohana's account. These directives were being sent to Defendant weeks before their most recent request on June 13, 2024 for leave under the Family and Medical Leave Act ("FMLA"). Defendant has utilized FMLA leave, which is their right, periodically since January 2024;

c. For weeks, they have been directed in writing to provide full administrative rights to Justin Drummond, Ohana's President, to Victor Brick, Ohana's CEO, and to Norris, the CFO, in addition to Mr. Brooks;

d. They have been directed in writing to provide full administrative rights to Phil Leadore, which Ohana engaged to assist with IT matters; and

e. They took action to lock Richard Hartman, Ohana's Vice President of Human Resources, out of his Ohana company email account and his Microsoft Teams account, right after Defendant received the notice from Mr. Hartman that they were suspended from employment.

16. Defendant's use of FMLA is not a legal basis for their failure to comply with the Company's previous directives or this Court's Order. In fact, Defendant fails to identify any legal basis for their refusal to comply with the TRO.

17. Moreover, Defendant's conduct is a violation of criminal law. Ohana is prepared to seek prosecution under MD. CODE ANN., CRIM. LAW., §7-302(C) should Defendant continue to act in direct dereliction of the TRO and their duties as an employee of Ohana.

Exhibit 9C

18. Pursuant to Rule 15-206(c)(1), Ohana, through its counsel, expressly states that it does not request incarceration of Defendant at this time.

WHEREFORE, for the foregoing reasons, Ohana requests entry of an Order:

A. Directing Defendant to personally appear in open court to show cause as to why they should not be held in contempt of this Court's June 17, 2024 TRO.

B. Requiring that, pursuant to Rule 15-206(d), a copy of this Petition for Civil Contempt and the Court's Order regarding the same be served on Defendant via email and first-class mail, postage prepaid to their addresses of record in this matter;

C. Directing that, pursuant to Rule 15-206(c)(2)(A), the alleged contemnor, Ryan Dillon-Capps, file an answer to this Petition for Constructive Civil Contempt within ten (10) days[1] of the service of the Court's Order;

D. Requiring Defendant to immediately comply with the TRO;

E. Awarding Ohana its reasonable attorneys' fees and costs incurred in preparing and prosecuting this Petition in an amount to be determined after the Court's ruling on entitlement to costs and attorney's fees; and

F. Any such other relief as justice and the nature of its cause may require.

June 20, 2024

Respectfully submitted,

/s/ Robert S. Brennen
Robert S. Brennen (AIS # 8712010068)
e-mail: RBrennen@milestockbridge.com
Stephen D. Frenkil (AIS # 7712010110)
e-mail: SFrenkil@milesstockbridge.com
Victoria K. Hoffberger (AIS # 1912170195)
e-mail: VHoffberger@milesstockbridge.com
MILES & STOCKBRIDGE P.C.

[1] There is a Preliminary Injunction hearing scheduled for June 26, 2024. While less than ten (10) days from the date of this filing, in order to promote judicial efficiency, Ohana requests that Dillon-Capps show cause as to why they should not be held in contempt at this hearing.

Exhibit 9C

100 Light Street
Baltimore, Maryland 21202
Telephone: (410) 727-6464
Facsimile: (410) 385-3700

Counsel for Plaintiff Ohana Growth Partners, LLC

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on June 20, 2024, a copy of the **Petition to Show Cause and for Constructive Civil Contempt** was sent via email to ryan@mxt3.com and served on via first-class mail, postage prepaid on:

Ryan Dillon-Capps
1334 Maple Avenue
Essex, Maryland 21221

/s/ Robert S. Brennen
Robert S. Brennen (AIS # 8712010068)

Exhibit 9C

OHANA GROWTH PARTNERS, LLC	**IN THE**
Plaintiff,	**CIRCUIT COURT**
vs.	**FOR**
RYAN DILLON-CAPPS	**BALTIMORE COUNTY**
Defendant.	**FILE NO.: C-03-CV-24-002264**

ORDER TO APPEAR AND SHOW CAUSE

Upon consideration of Ohana's Petition for Show Cause Order and Constructive Civil Contempt, and for good cause shown, it is this ____ day of ____________, 2024, hereby:

ORDERED that the Petition be, and hereby is, GRANTED; and it is further

ORDERED that Ohana shall appear before the Circuit Court for Baltimore County, Maryland on the ____ day of June, 2024, at ___ a.m./p.m. for a hearing at which Ryan Dillon-Capps shall show cause why they should not be held in contempt of this Court's June 17, 2024 Temporary Restraining Order.

____
Judge, Circuit Court for Baltimore County

Exhibit 9C

Case # C-03-CV-24-002264 - Ohana Growth Partners, LLC vs. Ryan

Envelope Information

Envelope Id	Submitted Date	Submitted User Name
16909122	6/20/2024 12:24 PM EST	rbrennen@milesstockbridge.com

Case Information

Location	Category	Case Type
Baltimore County Circuit Court	Civil	Injunction
Case Initiation Date	**Case #**	
6/14/2024	C-03-CV-24-002264	

Filings

Filing Type	Filing Code
EFileAndServe	Petition for Contempt/Enforcement

Filing Description
Petition to Show Cause and For Constructive Civil Contempt

Client Reference Number
119447-4

Courtesy Copies
kjedwards@milesstockbridge.com

Filing Status
Submitted

Lead Document

File Name	Description	Security	Download
Petition to Show Cause and for Contempt.pdf	Petition for Contempt/Enforcement		Original File

eService Details

Status	Name	Firm	Served	Date Opened
	S. Brennen	Miles & Stockbridge P.C.	Yes	Not Opened
Sent	Steven D. Frenkil	Miles & Stockbridge P.C.	Yes	6/20/2024 12:27 PM EST

Support

Exhibit 9C

Status	Name	Firm	Served	Date Opened
Sent	Victoria Klein	Miles & Stockbridge P.C.	Yes	Not Opened
Sent	Kim Edwards	Miles & Stockbridge P.C.	Yes	Not Opened

Filing Type
EFileAndServe

Filing Code
Proposed Order / Decree

Filing Description
Proposed Order

Client Reference Number
119447-4

Courtesy Copies
kjedwards@milesstockbridge.com

Filing Status
Submitted

Lead Document

File Name	Description	Security	Download
Proposed Order.pdf	Proposed Order / Decree		Original File

eService Details

Status	Name	Firm	Served	Date Opened
Sent	Steven D. Frenkil	Miles & Stockbridge P.C.	Yes	6/20/2024 12:27 PM EST
Sent	Victoria Klein	Miles & Stockbridge P.C.	Yes	Not Opened
Sent	Robert S. Brennen	Miles & Stockbridge P.C.	Yes	Not Opened
Sent	Kim Edwards	Miles & Stockbridge P.C.	Yes	Not Opened

Parties with No eService

Name	Address
Ryan Dillon-Capps	1334 Maple Avenue Essex Maryland 21221

Fees

Exhibit 9C

Petition for Contempt/Enforcement

Description	Amount
Filing Fee	$31.00
	Filing Total: $31.00

Proposed Order / Decree

Description	Amount
Filing Fee	$0.00
	Filing Total: $0.00

Total Filing Fee	$31.00
Payment Service Fee	$1.08
	Envelope Total: $32.08

Transaction Amount	$32.08		
Transaction Id	23341839		
Filing Attorney	Robert Brennen	**Order Id**	016909122-0
Transaction Response	Authorized		

Version: 2022.0.3.9946

Exhibit 10Q

amount shall be payable in the manner we determine. The foregoing sentence is not intended to cover enrollment fees or prorated fees for memberships with monthly and annual fees included in the EFT Dues Draft. You may only market paid-in-full memberships through programs or promotions that we authorize.

9.12 **RECIPROCAL MEMBERSHIP.** You must participate fully in any reciprocal access program (currently the Black Card program and Pre-Sale access program, as we may modify from time to time) and/or customer loyalty program(s) we may establish, in accordance with the policies and procedures set forth in the Operations Manual, through communications from us and as modified from time to time. You agree and acknowledge that for any reciprocal usage by **PLANET FITNESS** members of other franchisees, us or our Affiliates or when a person redeems any membership benefits or other customer loyalty program benefits at your BUSINESS, you are not entitled to reimbursement for membership fees or the cost of goods or services provided to the member as a reciprocal access member or under any customer loyalty program and that your BUSINESS benefits from this arrangement. Currently, (a) reciprocal access members of other **PLANET FITNESS** Businesses each have access to your BUSINESS up to ten (10) times per month and your reciprocal access members will each have access to other **PLANET FITNESS** Businesses up to ten (10) times per month and (b) all members of other nearby **PLANET FITNESS** Businesses in Pre-Sale will have full access to your BUSINESS during Pre-Sale and your members will have full access to other nearby **PLANET FITNESS** Businesses during your Pre-Sale. Subject to applicable law, we reserve the right to require you to charge a maximum or minimum day fee to reciprocal access members of other **PLANET FITNESS** Businesses visiting a **PLANET FITNESS** Business outside of the country in which such member's home is located.

9.13 **MEMBER TRANSFER POLICY AND COMPETITOR ACQUISITION.** You agree to comply with the member transfer policy as we establish from time to time. You acknowledge and agree that upon a transfer, the member's ongoing monthly dues and annual fees shall be transferred to the new location. If a membership is prepaid and is permitted to transfer pursuant to the member transfer policy, you agree to service the remaining prepaid term without compensation to you. Any acquisition of a Competitive Business (to convert to a **PLANET FITNESS** Business) or of membership lists or a group of members from a Competitive Business must be executed in accordance with the policies and procedures for the acquisitions of Competitive Businesses we may reasonably require and as set forth in the Operations Manual. You must ensure that any transfer of a membership to the BUSINESS is done in accordance with applicable law.

9.14 **DATA SECURITY AND DATA PRIVACY.**

(1) *Data Events.* You shall use your best efforts to protect your customers and the System, including your members, against a cyber-event including, without limitation, a data breach or other identity theft or theft, misuse, unauthorized access, or improper handling of personal or healthcare information (collectively, a "Data Event"). If you become aware that it is reasonably likely that a Data Event has occurred, regardless of whether such event affects only the BUSINESS, in addition to any obligations you may have under applicable law, you shall (i) notify us as soon as possible and, in any event, no later than within twenty-four (24) hours of becoming aware of the Data Event and (ii) promptly investigate the Data Event and remediate the source of any compromise or security breach at your expense. We reserve the right to perform and/or control all aspects of the response to such event to the maximum extent permitted by law including, without limitation, the investigation, containment and resolution of the event and all communications with the **PLANET FITNESS** franchise system, vendors and suppliers, members, law enforcement agencies, federal and state regulatory authorities, and the general public. In the event we elect to perform and/or control some or all aspects of the response to a Data Event you shall fully cooperate with all reasonable requests and inquiries and make all requested information, documents, systems, and personnel reasonably accessible and available. Our control of the response may potentially affect or interrupt operations of the

Exhibit 10Q

BUSINESS but does not create any additional rights for you, entitle you to damages or relieve you of your indemnification obligations pursuant to Article 18.4. Notwithstanding our right to perform and/or control all aspects of the response to a Data Event, we agree to make commercially reasonable efforts to coordinate such response with you and your insurance carrier(s) and to reasonably cooperate with your insurance carrier(s) regarding insurance coverage of such Data Event to the extent reasonably practicable under the circumstances. You are solely responsible for providing any legally required notices and credit and transaction monitoring services and any other response required under applicable law, unless otherwise directed by us in writing.

(2) *Data Security and Privacy Standards.* You shall establish physical, technical and administrative safeguards against the loss, theft, mishandling, or improper alteration, or disclosure of data and unauthorized access to your systems consistent with current industry standards, including, but not limited to, encryption and redaction practices. You shall at all times comply with: (a) the Payment Card Industry Data Security Standards, (b) the NACHA ACH Security Framework, (c) Payment Rules, (d) applicable laws and regulations relating to electronic payments, data and/or personal information, privacy, data security and security breaches including, but not limited to, if applicable, state consumer privacy laws and laws implementing the European General Data Protection Regulation and (e) our security policies and guidelines, all as may be amended from time to time ((a) through (e) collectively, “Data Rules”). You shall fully cooperate with us and our Affiliates in meeting our compliance obligations under applicable Data Rules and refrain from any action that may cause us or any of our Affiliates to violate any applicable Data Rule. You shall notify us immediately in the event you discover that you are not in compliance with the Data Rules. We may designate certain third-party consultant(s) to administer our data security program and evaluate your compliance with the aforementioned standards. You must meet promptly the reasonable requirements of any such consultant(s) and maintain those certifications of compliance that we deem appropriate in our reasonable discretion. We may require you to (a) use suppliers we designate or approve to provide data security or privacy services and/or audit your compliance with the Data Rules and (b) provide us with evidence of compliance with the Data Rules (including copies of any audits) promptly upon our request. You are expected to obtain independent advice from appropriate legal and security consultants (which may include consultants we require or designate) to ensure that you operate your BUSINESS at all times in full compliance with the Data Rules.

(3) *Limitations on Personal Data.* You agree to limit the collection of Personal Data to that which is reasonably necessary and proportionate to the operation of the BUSINESS in accordance with this Agreement, to provide all legally required notices to consumers at the time of such collection of Personal Data, and to not retain, use, process or disclose Personal Data for any other purpose. You will not sell, rent or license Personal Data and may not disclose or authorize access to Personal Data to third parties (except your affiliates that are developing or operating **PLANET FITNESS** businesses in the United States) without our prior written approval. You shall comply with this Article 9.14 with respect to all Personal Data.

9.15 TECHNOLOGY.

(1) *Technology Infrastructure.* You must have Internet access and an e-mail address. In addition to the requirements in Articles 4.5 and 4.6, you agree to purchase or lease, at your expense, such computer hardware, software, POS systems, billing systems, related accessories, network accessories, peripheral equipment, and services as we may specify for the purpose of, among other functions, recording financial and customer data, communicating with us, and operating the BUSINESS. You agree, at

Exhibit 10Q

your expense, to establish the information technology infrastructure and processes that we require, regarding, without limitation, your computer systems, payment systems, customer systems, internal and external networks, back-up systems, mobile devices, and any other network access points. You agree, at your expense, to purchase such installation and support services as we may reasonably require, to keep all equipment, systems, and devices in good maintenance and repair, and to promptly update or install such additions, changes, modifications, substitutions or replacements as we direct. You agree that you will comply strictly with our standards and specifications for all equipment and processes associated with your computer systems and technology. You shall comply with our reasonable polices with respect to the use or download of software or SaaS/PaaS solutions in connection with the BUSINESS.

(2) *New Initiatives and Standards.* You acknowledge and agree that changes to technology are dynamic and not predictable within the Term of this Agreement. In order to provide for inevitable but unpredictable changes to technological needs and opportunities, and to protect against new and emerging technological risks, you and we agree that we shall have the right to establish, through our Operations Manual, reasonable new standards and initiatives for the implementation of technology in the System; and you agree that you shall abide by those reasonable new standards established by us, at your expense. You may be required to invest in and implement new technology initiatives at your own expense including, but not limited to, membership offerings, acceptance of new forms of payment, monitors, music, Internet TV broadcast, delivery of digital content related to the BUSINESS, software management applications, surveillance system, e-learning, and software applications designed to better manage business functions and control costs. We may designate the supplier you use for any goods and services associated with these and other initiatives. You further acknowledge and agree that such new standards and initiatives may require an investment in, without limitation, new hardware, software, training, procedures, vendors, and/or services. We will consult, in an advisory capacity, with the recognized franchisee association (or the appropriate subcommittee thereof) on issues related to new technology standards or initiatives that would require substantial capital expenditures by you.

(3) *Uniform Applicability.* We agree that the requirements in this Article 9.15 and the standards and specifications referenced hereunder also are applicable to the **PLANET FITNESS** Businesses owned by our Affiliates and by us.

9.16 DESIGNATED FRANCHISE PORTAL. You agree to actively use and monitor our then current Designated Franchise Portal in connection with the development and operation of your BUSINESS. You shall be deemed to be "actively using and monitoring" the Designated Franchise Portal if you, or any of your Owners, Responsible Owners, Approved Operators, and/or managers log in to the Designated Franchise Portal at least once per week.

10. MARKETING.

10.1 NATIONAL ADVERTISING.

(1) *Establishment of NAF; Ad Fees.* Recognizing the value of advertising and marketing to the goodwill and public image of **PLANET FITNESS** Businesses and the **PLANET FITNESS** brand, we have established and administer a National Advertising Fund ("NAF") for the creation and development of marketing, advertising, digital, and related programs and materials, including electronic, print and Internet media as well as the planning and purchasing of national and/or regional (which, for clarity, may include one (1) or more designated market areas) network advertising to promote and enhance the **PLANET FITNESS** brand in such manner

Exhibit 10W

your landlord, System suppliers or that we are otherwise required to pay in order to assume lawful occupancy of the Location and operation of the BUSINESS and the costs of remedying any material unaddressed noncompliance with our standards, unless such owed amounts are already reflected in the purchase price.

(7) Instruments. At the closing, you agree to deliver instruments transferring:

(a) good and merchantable title to the assets purchased, free and clear of all liens and encumbrances (other than liens and security interests acceptable to us, if any), with all sales and other transfer taxes paid by you;

(b) all licenses and permits of the BUSINESS which may be assigned or transferred; and

(c) the leasehold interest in the Location and improvements thereon.

(8) Escrow. If you cannot deliver clear title to all of the purchased assets, or if there are other unresolved issues, the closing of the sale will, at our election, be accomplished through an escrow arrangement with an independent escrow agent selected by us.

(9) Releases. In connection with the closing of the sale, you and your Owners agree to execute General Releases.

(10) Operations. We may, but are not obligated to, assume operations of the BUSINESS as provided under Article 15.6 hereof, from the date of the Purchase Notice until closing. You must cooperate with and facilitate such assumption.

16.14 **CONTINUING OBLIGATIONS**. All of our and your (and your Owners' and Affiliates') obligations which expressly or by their nature survive the expiration or termination of this Agreement will continue in full force and effect subsequent to and notwithstanding its expiration or termination and until they are satisfied in full or by their nature expire.

17. SECURITIES OFFERINGS.

17.1 **SECURITIES OFFERINGS**. Neither you nor any of your Owners may issue or sell, or offer to issue or sell, any of your securities or any securities of any of your Affiliates, if (1) such securities would be required to be registered pursuant to the Securities Act of 1933, as amended; (2) such securities would be owned by more than thirty five (35) persons; or (3) after such issuance or sale, you or such Affiliate would be required to comply with the reporting and information requirements of the Securities Exchange Act of 1934, as amended. Other offers, issuances or sales by you or your Owners of any of your securities or any securities of any of your Affiliates are subject to (1) our prior consent, such consent not to be unreasonably withheld, conditioned or delayed and (2) your compliance with all applicable laws and all of our requirements and restrictions concerning use of information about us and our Affiliates. If such proposed offering is either (i) a customary employee equity incentive or (ii) an equity issuance in connection with an additional capital contribution by an existing Owner, our consent under this Article 17.1 will not be required (although such proposed offering may be subject to Article 13 hereof). Any proposed private placement of your or of your Affiliate's securities must be approved by us. For any proposed securities offering approved in principle by us, you shall submit to us for our prior review all materials required by applicable law for the offering. No such materials shall be submitted to a government agency or to prospective investors unless and until we have furnished our written approval. No offering materials shall imply, by use of the Marks or otherwise, that we, our Affiliates, or our respective directors, officers, employees, shareholders, or agents are participating as an underwriter, issuer, or offeror of securities of either you or us, or that we have approved the offering prospectus or any other aspect of the offering. Any review by us of the offering materials or the information included therein shall be

Exhibit 10W

conducted solely for our benefit to determine their conformance with our internal policies, and not to benefit or protect any other person. Such review by us does not constitute, nor shall you or anyone acting on your behalf suggest that our review constitutes an approval, endorsement, acceptance, or adoption of any representation, warranty, covenant, or projection contained in the materials reviewed; and the offering documents shall include legends and statements, in the form and manner specified by us, disclaiming our liability for, or involvement in, the transaction described in the offering documents. You and other participants in the offering, must fully indemnify, defend and hold harmless us, our Affiliates and our respective directors, officers, employees, shareholders, and agents from any and all losses and expenses that arise directly or indirectly from, as a result of, or in connection with the offering. For any proposed offering, you shall reimburse our out-of-pocket costs (including the costs of our legal and accounting advisors) to review the materials when incurred. In addition, for any proposed offering that requires our consent under this Article 17.1, we may require you to pay us a non-refundable fee of up to the lesser of (a) one percent (1%) of the capital to be raised in the offering or (b) One Hundred Thousand U.S. Dollars ($100,000), at the time that you submit materials for review by us. Such fee may be charged only once to you and your Affiliates per offering, and will not be charged on a per-Franchise Agreement basis. You shall give us written notice at least ninety (90) days prior to the date of commencement of any offering or other transaction covered by this Article 17.1. Any such offering may be subject to our right of first refusal as provided in Article 13.8 hereof.

18. RELATIONSHIP OF THE PARTIES AND INDEMNIFICATION.

18.1 **INDEPENDENT CONTRACTORS.** Neither this Agreement nor the dealings of the parties pursuant to this Agreement shall create any fiduciary relationship or any other relationship of trust or confidence between the parties hereto. Furthermore, you and we acknowledge that this Agreement does not create any labor or employment relationship between you and us, nor between your and our employees, contractors, representatives and agents and that you are acting within the ordinary course of your business. The parties hereto, as between themselves, are and shall be independent contractors. You must conspicuously identify yourself in all dealings with customers, lessors, contractors, suppliers, public officials, employees and others as the owner of your BUSINESS and must provide written notice to all employees identifying yourself as a separate and distinct business from us, with such notice being affirmatively acknowledged by each of your employees in a form we specify in the Operations Manual or otherwise in writing from time to time. You agree to always indicate your status as an independent contractor and franchisee on any document or information released by you or any agreement you enter into in connection with the BUSINESS and to place such other notices of independent ownership on such forms, business cards, stationery, advertising and other materials as we may require from time to time. Further, you will display the following notice in a prominent place at the BUSINESS: ***"This Planet Fitness is a franchise of Planet Fitness Franchising LLC and is independently owned and operated."***

18.2 **NO LIABILITY FOR ACTS OF OTHER PARTY.** You agree not to employ any of the Marks in signing any contract or applying for any license or permit, or in a manner that may result in our liability for any of your indebtedness or obligations. Neither we nor you will be obligated by or have any liability under any agreements or representations made by the other that are not expressly authorized in writing, except as we may be authorized to do under this Agreement. We will not be obligated for any damages of any nature whatsoever to any person or property arising directly or indirectly out of the operation of your BUSINESS.

18.3 **TAXES.** We will have no liability for any sales, use, service, occupation, employment related, excise, gross receipts, income, property or other taxes, whether levied upon you or the BUSINESS, in connection with the business you conduct (except any taxes we are required by law to collect from you with respect to purchases from us). Payment of all such taxes is your sole responsibility. Further, you will pay all state and local taxes, including, without limitation, sales, use, service, occupation, employment related, excise, gross receipts, income, property or other taxes that may be imposed on us as a result of our receipt or accrual of the Initial Franchise Fee, Royalty fees, advertising fees, extension fees, and all other fees that are referenced in this Agreement or in the

Exhibit 10W

Methods of Operation, whether assessed against you through withholding or other means or whether paid by us directly, unless the tax is credited against income tax otherwise payable by us. In such event, you will pay to us (or to the appropriate governmental authority) such additional amounts as are necessary to provide us, after taking such taxes into account (including any additional taxes imposed on such additional amounts), with the same amounts that we would have received or accrued had such withholding or other payment, whether by you or by us, not been required. Notwithstanding anything to the contrary in this Agreement, this provision does not apply to taxes imposed on us by the state or municipality where we have our principal place of business.

18.4 **INDEMNIFICATION. IN ADDITION TO YOUR OTHER INDEMNIFICATION OBLIGATIONS SET FORTH IN THIS AGREEMENT, YOU, AND EACH OF THE GUARANTORS, AGREE THAT YOU SHALL, AT ALL TIMES, INDEMNIFY, EXCULPATE, DEFEND AND HOLD HARMLESS, TO THE FULLEST EXTENT PERMITTED BY LAW, US, OUR SUCCESSORS, ASSIGNS, AND AFFILIATES (INCLUDING, BUT NOT LIMITED TO, PLANET FITNESS DISTRIBUTION LLC), AND THE RESPECTIVE OFFICERS, DIRECTORS, SHAREHOLDERS, AGENTS, REPRESENTATIVES, INDEPENDENT CONTRACTORS, SERVANTS, AND EMPLOYEES OF EACH OF THEM (THE "INDEMNIFIED PARTIES") FROM ALL LOSSES AND EXPENSES INCURRED IN CONNECTION WITH ANY ACTION, SUIT, PROCEEDING, CLAIM, DEMAND, INVESTIGATION, OR INQUIRY (FORMAL OR INFORMAL), OR ANY SETTLEMENT THEREOF, WHICH ARISES OUT OF OR IS BASED UPON ANY OF THE FOLLOWING: (A) THE INFRINGEMENT, ALLEGED INFRINGEMENT OR ANY OTHER VIOLATION BY YOU, YOUR GUARANTORS OR OWNERS OF ANY PATENT, MARK, COPYRIGHT, OR OTHER PROPRIETARY RIGHT OWNED OR CONTROLLED BY THIRD PARTIES DUE TO YOUR UNAUTHORIZED USE OF ALL OR ANY PORTION OF THE MARKS AND/OR SYSTEM OR YOUR USE OF ANY MARKS OR OTHER INTELLECTUAL PROPERTY NOT LICENSED FROM US; (B) THE VIOLATION, BREACH, OR ASSERTED OR ALLEGED VIOLATION OR BREACH BY YOU, YOUR GUARANTORS OR OWNERS OF ANY FEDERAL, STATE, OR LOCAL LAW, REGULATION, RULING OR INDUSTRY STANDARD; (C) THE VIOLATION OR BREACH OR ALLEGED VIOLATION OR BREACH BY YOU OR BY YOUR GUARANTORS OR OWNERS OF ANY WARRANTY, REPRESENTATION, AGREEMENT, OR OBLIGATION OF THIS AGREEMENT OR IN ANY OTHER AGREEMENT BETWEEN YOU AND US OR OUR AFFILIATES ARISING OUT OF OR RELATED TO THIS AGREEMENT; (D) ANY DATA EVENT OR ALLEGED DATA EVENT ARISING FROM THE BUSINESS OR FROM THE ACTIONS OR INACTIONS OF YOU OR YOUR PERSONNEL; OR (E) ACTS, ERRORS, OR OMISSIONS OR ALLEGED ACTS, ERRORS OR OMISSIONS OF YOU, ANY OF YOUR AFFILIATES, ANY OF YOUR OWNERS, OFFICERS, DIRECTORS, SHAREHOLDERS, AGENTS, REPRESENTATIVES, INDEPENDENT CONTRACTORS, AND EMPLOYEES OF YOU AND YOUR AFFILIATES IN CONNECTION WITH THE ESTABLISHMENT AND OPERATION OF THE BUSINESS, INCLUDING, BUT NOT LIMITED TO, ANY ACTS, ERRORS, OR OMISSIONS OF ANY OF THE FOREGOING IN THE OPERATION OF ANY MOTOR VEHICLE OR IN THE ESTABLISHMENT OR IMPLEMENTATION OF SECURITY FOR THE BUSINESS; UNLESS (AND THEN ONLY TO THE EXTENT THAT) THE CLAIMS, OBLIGATIONS, AND DAMAGES ARE DETERMINED TO BE CAUSED SOLELY BY THE INDEMNIFIED PARTY'S NEGLIGENCE OR WILLFUL MISCONDUCT ACCORDING TO A FINAL, UNAPPEALABLE RULING ISSUED BY A COURT OR ARBITRATOR WITH COMPETENT JURISDICTION. FOR PURPOSES OF THIS INDEMNIFICATION, "LOSSES AND EXPENSES" INCLUDE ALL OBLIGATIONS, DAMAGES (ACTUAL, CONSEQUENTIAL OR OTHERWISE) AND COSTS INCURRED IN THE DEFENSE OF ANY CLAIM AGAINST ANY OF THE INDEMNIFIED PARTIES, INCLUDING, WITHOUT LIMITATION, REASONABLE ACCOUNTANTS', ARBITRATORS', ATTORNEYS' AND EXPERT WITNESS FEES, COSTS OF INVESTIGATION AND PROOF OF FACTS, COURT COSTS, OTHER EXPENSES OF LITIGATION, ARBITRATION OR ALTERNATIVE DISPUTE**

Exhibit 10W

RESOLUTION, SETTLEMENT COSTS, AND TRAVEL AND LIVING EXPENSES. WE HAVE THE RIGHT TO DEFEND ANY SUCH CLAIM AGAINST US AT YOUR EXPENSE WITH COUNSEL WE SELECT. YOU SHALL PROVIDE THE ADDITIONAL COOPERATION AND ASSISTANCE THAT WE REQUEST IN ORDER TO RELEASE THE INDEMNIFIED PARTIES FROM LIABILITY FOR INDEMNIFIABLE LOSSES AND EXPENSES HEREUNDER. THIS INDEMNITY WILL CONTINUE IN FULL FORCE AND EFFECT SUBSEQUENT TO AND NOTWITHSTANDING THE EXPIRATION OR TERMINATION OF THIS AGREEMENT.

18.5 **MITIGATION NOT REQUIRED.** Under no circumstances will we or any other Indemnified Party be required to seek recovery from any insurer or other third party, or otherwise to mitigate our, their or your losses and expenses, in order to maintain and recover fully a claim against you. You agree that a failure to pursue such recovery or mitigate a loss will in no way reduce or alter the amounts we or another Indemnified Party may recover from you.

18.6 **NOTIFICATION OF ADVERSE ACTION.** You shall promptly notify us in writing of (a) a notice of violation or alleged violation of any law, ordinance or regulation that, if not addressed, would be reasonably expected to have a material effect on the BUSINESS, (b) a material threat that is likely to result in the commencement of any action, suit, proceeding or investigation, (c) the actual commencement of any such action, suit, proceeding or investigation, or (d) the issuance of any order, writ, injunction, award, or decree of any court, agency, or other governmental instrumentality, in each case, against you, any of your Affiliates, us, or our Affiliates, that relates to the BUSINESS, or which may adversely affect the development, occupancy or operation of the BUSINESS or your financial condition. Upon our request, you shall furnish to us within five (5) Business Days after receipt thereof, a copy of any notices, subpoenas, or other initial pleadings served upon or received by you in connection with such proceeding, provide us with updates of substantive developments and otherwise cooperate with us in monitoring the progress of any such proceeding. You shall furnish to us within two (2) Business Days after receipt thereof, a copy of any material violation or citation which indicates your violation of any law, regulation, or ordinance in the operation of the BUSINESS, of your Lease, or of any alleged health or safety code violation from any governmental agency that, if not addressed, would be reasonably expected to have a material effect on the BUSINESS. You shall immediately notify us of any event or circumstance related to the BUSINESS that is reasonably likely to attract material negative media or regulatory attention or might be reasonably expected to negatively impact the reputation of the **PLANET FITNESS** brand or the goodwill associated with the Marks.

19. ENFORCEMENT AND MISCELLANEOUS MATTERS.

19.1 **SEVERABILITY AND SUBSTITUTION OF VALID PROVISIONS.** Except as expressly provided to the contrary herein, each provision of this Agreement, and any portion thereof, will be considered severable and if, for any reason, any such provision is held to be invalid or contrary to or in conflict with any applicable present or future law or regulation in a final, unappealable ruling issued by any court, agency or tribunal with competent jurisdiction in a proceeding to which we are a party, that ruling will not impair the operation of, or have any other effect upon, such other portions of this Agreement as may remain otherwise intelligible, which will continue to be given full force and effect and bind the parties hereto, although any portion held to be invalid will be deemed not to be a part of this Agreement from the date the time for appeal expires, if you are a party thereto, otherwise upon your receipt from us of a notice of non-enforcement thereof.

19.2 **LESSER COVENANT ENFORCEABLE.** If any covenant herein which restricts competitive activity is deemed unenforceable by virtue of its scope in terms of area, business activity prohibited and/or length of time, but would be enforceable by reducing any part or all thereof, you and we agree that such covenant will be enforced to the fullest extent permissible under the laws and public policies applied in the jurisdiction whose law is applicable to the validity of such covenant.

Exhibit 10W

19.3 **GREATER NOTICE.** If any applicable and binding law or rule of any jurisdiction requires a greater prior notice than is required hereunder of the termination of this Agreement or of our refusal to enter into a successor franchise agreement, or the taking of some other action not required hereunder, or if, under any applicable and binding law or rule of any jurisdiction, any provision of this Agreement or any part of the mandatory Methods of Operation is invalid or unenforceable the prior notice and/or other action required by such law or rule will be substituted for the comparable provisions hereof, and we will have the right to modify such invalid or unenforceable provision or unenforceable part of this Agreement or the Operations Manual or any part of the mandatory Methods of Operation to the extent required to be valid and enforceable. You agree to be bound by any promise or covenant imposing the maximum duty permitted by law which is subsumed within the terms of any provision hereof as though it were separately articulated in and made a part of this Agreement, that may result from striking from any of the provisions hereof, or any part of the mandatory Methods of Operation, any portion or portions which a court or arbitrator may hold to be unenforceable in a final decision to which we are a party, or from reducing the scope of any promise or covenant to the extent required to comply with such a court order or arbitration award. Such modifications to this Agreement will be effective only in such jurisdiction, unless we elect to give them greater applicability, and will be enforced as originally made and entered into in all other jurisdictions.

19.4 **WAIVER OF OBLIGATIONS.** We and you may by written instrument unilaterally waive or reduce any obligation of or restriction upon the other under this Agreement, effective upon delivery of written notice thereof to the other or such other effective date stated in the notice of waiver. Any waiver we grant will be without prejudice to any other rights we may have, will be subject to our continuing review and may be revoked at any time and for any reason, effective upon delivery to you of ten (10) days' prior written notice. We and you will not be deemed to have waived or impaired any right, power or option reserved by this Agreement (including without limitation the right to demand exact compliance with every term, condition and covenant herein or to declare any breach thereof to be a default and to terminate this Agreement prior to the expiration of its term) by virtue of: any custom or practice at variance with the terms hereof; our or your failure, refusal or neglect to exercise any right under this Agreement or to insist upon exact compliance by the other with our and your obligations hereunder including without limitation the mandatory Methods of Operation; our waiver, forbearance, delay, failure, or omission to exercise any right, power or option whether of the same, similar or different nature with respect to other **PLANET FITNESS** Businesses; the existence of other franchise agreements for **PLANET FITNESS** Businesses which contain different provisions from those contained herein; or our acceptance of any payments due from you after any breach of this Agreement. We may adopt policies from time to time to guide our decision making, promote consistency and improve or protect the System. Such policies shall not be binding on us and are subject to change. No special or restrictive legend or endorsement on any check or similar item given to us will constitute a waiver, compromise, settlement or accord and satisfaction. We are authorized to remove or obliterate any legend or endorsement, and such legend or endorsement will have no effect.

19.5 **FORCE MAJEURE.** Neither we nor you will be liable for loss or damage or deemed to be in breach of this Agreement if our or your failure to perform our or your obligations is not our or your fault and results from (each, a "Force Majeure Event"):

(1) transportation shortages, inadequate supply of equipment, products, merchandise, supplies, labor, material or energy or the voluntary foregoing of the right to acquire or use any of the foregoing in order to accommodate or comply with the orders, regulations, or instructions of any federal, state or municipal government or any department or agency thereof;

(2) hurricanes, earthquakes, or other acts of nature;

(3) fires, strikes, embargoes, war or riot; or

(4) any other similar event or cause beyond the reasonable control of the applicable party.

Exhibit 10W

Notwithstanding the above, lack of funds and economic conditions shall not constitute a Force Majeure Event hereunder. Any delay resulting from a Force Majeure Event will extend performance accordingly or excuse performance, in whole or in part, as may be reasonable, except that a Force Majeure Event will not extend the timeline for or excuse any payment obligations to us or our Affiliates hereunder. If we send you a Notice of Default, and you believe a Force Majeure Event has occurred which relates to the applicable Event of Default, you must promptly notify us and include in such notice a description of the Force Majeure Event, its impact on your obligations to us and the estimated duration of impact.

19.6 **OUT-OF-STOCK AND DISCONTINUED.** We are not liable to you for any loss or damage, or deemed to be in breach of this Agreement, if we cannot deliver, or cause to be delivered, or if our Affiliates or designated sources or Approved Suppliers cannot deliver, all of your orders for products, merchandise, equipment, supplies, etc., where such things are out-of-stock or discontinued.

19.7 **COSTS AND ATTORNEYS' FEES.** If we incur expenses in connection with your failure to pay when due amounts owed to us or to submit when due any reports, information or supporting records or otherwise to comply with this Agreement, you agree to reimburse us for any of the costs and expenses which we incur, including, without limitation, reasonable accounting, attorneys', and related fees. The prevailing party in any action or proceeding arising under, out of, in connection with, or in relation to this Agreement will be entitled to recover its reasonable costs and expenses (including attorneys' fees, arbitrator's fees and expert witness fees, costs of investigation and proof of facts, court costs, and other arbitration or litigation expenses) incurred in connection with the claims on which it prevailed. If any party does not participate in mediation after receiving a written demand to do so, as required hereunder, such party will be required to pay the reasonable costs and expenses (including attorneys' fees, arbitrator's fees and expert witness fees, costs of investigation and proof of facts, court costs, and other arbitration or litigation expenses) of the other party incurred after such party's failure to participate in the mediation. If you have requested this Agreement at a time when we are actively pursuing, but do not have an active franchise registration in an applicable jurisdiction, if you request a change to this Agreement after signing, or if you request additional documents (amendments, assignments, tri-party agreements, lender consents or comfort letters, etc.), and, in connection with our fulfillment of such request, we incur third-party costs or pay a filing fee, we may require you to pay or reimburse such reasonable costs and fees.

19.8 **RIGHTS OF PARTIES ARE CUMULATIVE.** Our and your rights hereunder are cumulative, and no exercise or enforcement by us or you of any right or remedy hereunder will preclude our or your exercise or enforcement of any other right or remedy hereunder which we or you are entitled by law to enforce.

19.9 **DISPUTE RESOLUTION.**

(1) Mediation. Except as provided in Article 19.9(3), prior to filing any demand for arbitration, the parties agree to mediate any dispute, controversy or claim between and among the parties and any of our or your Affiliates, officers, directors, shareholders, members, guarantors, employees or owners arising under, out of, in connection with or in relation to this Agreement, any Lease for your BUSINESS, any loan or other finance arrangement between us or our Affiliates and you, the parties' relationship, your BUSINESS, or any System standard in accordance with the following procedures:

(a) The party seeking mediation must commence mediation by sending the other party, in accordance with Article 20, a written notice of its request for mediation headed "Notification of Dispute." The Notification of Dispute will specify, to the fullest extent possible, the party's version of the facts surrounding the dispute; the amount of damages and the nature of any injunctive or other relief such party claims. The party (or parties as the case may be) receiving a Notification of Dispute will respond within twenty (20) days after receipt thereof, in accordance

Exhibit 10W

with Article 20, stating its version of the facts and, if applicable, its position as to damages sought by the party initiating the dispute procedure; provided, however, that if the dispute has been the subject of a Notice of Default given under Article 15 of this Agreement, the other party will respond within ten (10) Business Days.

(b) Upon receipt of a Notification of Dispute and response under Article 19.9(1)(a), the parties will endeavor, in good faith, to resolve the dispute outlined in the Notification of Dispute and response. If the parties have been unable to resolve a dispute outlined in a Notification of Dispute or a response thereto within twenty (20) days after receipt of the response, either party may initiate a mediation procedure with the American Arbitration Association ("AAA"), pursuant to its Commercial Mediation Procedures (the "Procedures"). The parties must select a mediator either jointly or as provided in the Procedures.

(c) All mediation sessions will occur in Portsmouth, New Hampshire (or in the city of our then-current headquarters, if our headquarters are no longer in New Hampshire), and must be attended by your Responsible Owner (and any other persons with authority to settle the dispute on your behalf) and our representative(s) who is/are authorized to settle the dispute. The parties may be represented by counsel at the mediation. The parties agree to participate in the mediation proceedings in good faith and with the intention of resolving the dispute if at all possible within ninety (90) days of the notice from the party seeking to initiate the mediation procedures. If the dispute is not resolved within ninety (90) days, any party may initiate an arbitration pursuant to Article 19.9(2). In addition, if the party receiving notice of mediation has not responded within five (5) days of delivery of the notice or a party fails to participate in the mediation, this Article 19.9(1) will no longer be applicable and the other party can pursue arbitration. The parties shall split equally the costs of the mediator. Each party must pay its own fees and expenses incurred in connection with the mediation. The mediation proceeding and any negotiations and results thereof will be treated as a compromise settlement negotiation and the entire process is confidential, except as otherwise expressly provided by applicable law. At least five (5) days prior to the initial mediation session, each party must deliver a written statement of positions.

(2) Arbitration. Except as provided in Article 19.9(3), any dispute, controversy or claim between you and us and any of our or your Affiliates, officers, directors, shareholders, members, guarantors, employees or owners arising under, out of, in connection with or in relation to this Agreement, any Lease for your BUSINESS, any loan or other finance arrangement between us or our Affiliates and you, the parties' relationship, your BUSINESS, or any System standard or the scope of validity of the arbitration obligation under this Article not resolved by mediation must be submitted to binding arbitration in accordance with the Federal Arbitration Act. The arbitration will be administered by the AAA pursuant to its Commercial Arbitration Rules then in effect by one arbitrator.

(a) In connection with any arbitration proceeding, each party will submit or file any claim which would constitute a compulsory counterclaim (as defined by the then-current Rule 13 of the Federal Rules of Civil Procedure) within the same proceeding as the claim to which it relates. Any such claim not submitted or filed in such proceeding will be barred.

(b) Any arbitration must be on an individual basis only as to a single Franchise Group (and not as or through an association) and the parties and the arbitrator will have no authority or power to proceed with any claim on a class-wide basis or otherwise to join or consolidate any claim with any claim or any other proceeding involving third parties or any other Franchise Group. If a court or arbitrator determines that

Exhibit 10W

this limitation on joinder of or class-wide claims is unenforceable, then the agreement to arbitrate the dispute will be null and void and the parties must submit all claims to the jurisdiction of the courts, in accordance with Article 19.11.

(c) The arbitration must take place in Portsmouth, New Hampshire (or in the city of our then-current headquarters, if our headquarters are no longer in New Hampshire).

(d) The arbitrator must follow the law and not disregard the terms of this Agreement. The arbitrator may not consider any settlement discussions or offers that might have been made by either you or us. The arbitrator may not under any circumstance (a) stay the effectiveness of any pending termination of this Agreement, (b) assess punitive or exemplary damages, (c) certify a class or a consolidated action, or (d) make any award which extends, modifies or suspends any lawful term of this Agreement or any reasonable standard of business performance that we set. If the arbitrator determines that any contractual limitations period provided for in this Agreement is not applicable or enforceable, then the parties agree to be bound by the provision of any statute of limitations which would otherwise be applicable to the controversy, dispute or claim which is the subject of any arbitration proceeding initiated hereunder. The arbitrator will decide any factual, procedural, or legal questions relating in any way to the dispute between the parties, including, but not limited to: any decision as to whether this Article 19.9 is applicable and enforceable as against the parties, subject matter, timeliness, scope, remedies, unconscionability, and any alleged fraud in the inducement.

(e) Other than as may be required by law, the entire arbitration proceedings (including, but not limited to, any rulings, decisions or orders of the arbitrator), will remain confidential and will not be disclosed to anyone other than the parties to this Agreement.

(f) We reserve the right, but have no obligation, to advance your share of the costs of any arbitration proceeding in order for such arbitration proceeding to take place and by doing so will not be deemed to have waived or relinquished our right to seek recovery of those costs in accordance with Article 19.7 or 19.9(4).

(3) Injunctive Relief/No Waiver of Arbitration. Notwithstanding Articles 19.9(1) and 19.9(2) of this Agreement, either party shall have the right to request injunctive relief (without any requirement to post a bond) from any court of competent jurisdiction, including, without limitation, application for judicial relief to protect against trademark infringement, unauthorized use of trademark, loss of possession of real or personal property, violations of non-competition or confidentiality obligations, termination of this Agreement, or to maintain the efficacy of an ongoing arbitration, and that such request shall not constitute a waiver of the moving party's right to demand arbitration of any dispute pursuant to Article 19.9(2) and its subparts.

(4) Survival. The provisions of this Article 19.9 are intended to benefit and bind certain third party non-signatories and will continue in full force and effect subsequent to and notwithstanding the expiration or termination of this Agreement.

(5) Tolling of Statute of Limitations. All applicable statutes of limitation and defenses based on the passage of time are tolled while the dispute resolution procedures in this Article 19.9 are pending. The parties will take such action, if any, required to effectuate such tolling.

Exhibit 10W

(6) Performance to Continue. Each party must continue to perform its obligations under this Agreement pending final resolution of any dispute pursuant to this Article 19.9, unless to do so would be impossible or impracticable under the circumstances.

(7) Conflict. If there is a dispute between us and you and/or your affiliates involving this Agreement along with other Franchise Agreements between such parties, and those Franchise Agreements contain inconsistent dispute resolution provisions, then the procedural aspects of the dispute resolution provisions of the most recent Franchise Agreement, including, but not limited to, venue, and mediation and arbitration process, shall apply to the dispute in lieu of the provisions of Articles 19.9-19.12 hereof, unless this Agreement is the most recent Franchise Agreement, in which case the foregoing Articles shall apply to the dispute.

19.10 **GOVERNING LAW.** All matters relating to arbitration will be governed by the Federal Arbitration Act (9 U.S.C. §§ 1 *et. seq.*). Except to the extent governed by the Federal Arbitration Act as required hereby, the United States Trademark Act of 1946 (Lanham Act, 15 U.S.C. §§ 1051 *et* *seq.*) or other federal law, this Agreement, the franchise and all claims arising from the relationship between us and you will be governed by the laws of New Hampshire, without regard to its conflict of laws principles, except that any law regulating the sale of franchises or governing the relationship of a franchisor and its franchisee will not apply unless jurisdictional requirements are met independently without reference to this Article.

19.11 **CONSENT TO JURISDICTION.** Subject to Article 19.9, you and your Owners agree that we may institute any action or seek injunctive relief against you or your Owners in any state or federal court of general jurisdiction in New Hampshire or the county in which Franchisee is domiciled, or the county in which the Location is located, and you (and each Owner) irrevocably submit to the jurisdiction of any such courts and waive any objection you (or such Owner) may have to either the jurisdiction of or venue in such courts.

19.12 **WAIVER OF PUNITIVE DAMAGES, JURY TRIAL AND CLASS ACTIONS. EXCEPT WITH RESPECT TO YOUR OBLIGATION TO INDEMNIFY US PURSUANT TO ARTICLE 18.4 AND CLAIMS WE BRING AGAINST YOU FOR YOUR UNAUTHORIZED USE OF THE MARKS OR UNAUTHORIZED USE OR DISCLOSURE OF ANY CONFIDENTIAL INFORMATION OR BUSINESS INFORMATION, WE AND YOU AND YOUR OWNERS WAIVE TO THE FULLEST EXTENT PERMITTED BY LAW ANY RIGHT TO OR CLAIM FOR ANY PUNITIVE OR EXEMPLARY DAMAGES AGAINST THE OTHER AND AGREE THAT, IN THE EVENT OF A DISPUTE BETWEEN US, THE PARTY MAKING A CLAIM WILL BE LIMITED TO EQUITABLE RELIEF AND TO RECOVERY OF ANY ACTUAL DAMAGES IT SUSTAINS. WE AND YOU IRREVOCABLY WAIVE, TO THE FULLEST EXTENT PERMITTED BY LAW, TRIAL BY JURY IN ANY ACTION, PROCEEDING OR COUNTERCLAIM, WHETHER AT LAW OR IN EQUITY, BROUGHT BY EITHER OF US. THIS WAIVER IS EFFECTIVE EVEN IF A COURT OF COMPETENT JURISDICTION DECIDES THAT THE ARBITRATION PROVISION IN THIS ARTICLE 19 IS UNENFORCEABLE. WE EACH WAIVE TO THE FULLEST EXTENT POSSIBLE UNDER THE LAW OUR RESPECTIVE RIGHTS TO BRING AGAINST THE OTHER OR ANY AFFILIATE OR THE OTHER ANY CLAIMS DENOMINATED AS A CLASS ACTION, CONSOLIDATED ACTION, OR JOINT ACTION, WHETHER OR NOT PERMITTED UNDER APPLICABLE COURT RULES. EACH PARTY ACKNOWLEDGES THAT IT HAS HAD A FULL OPPORTUNITY TO CONSULT WITH COUNSEL CONCERNING THIS WAIVER, AND THAT THIS WAIVER IS INFORMED, VOLUNTARY, INTENTIONAL, AND NOT THE RESULT OF UNEQUAL BARGAINING POWER.**

19.13 **BINDING EFFECT.** This Agreement is binding upon us and you and our respective executors, administrators, heirs, beneficiaries, assigns and successors in interest and may not be modified

Exhibit 10W

except in accordance with Article 19.21 hereof; provided, however, we may unilaterally modify the Operations Manual.

19.14 **APPROVAL AND CONSENT.** Whenever our prior written approval or consent is required hereunder, you agree to submit to us a timely written request for such consent or approval. Except where this Agreement expressly obligates us reasonably to approve or not unreasonably to withhold our approval of any of your actions or requests, we have the absolute right to refuse any request you make or to withhold our approval of any of your proposed or effected actions that require our approval.

19.15 **HEADINGS; CONSTRUCTION.** The headings of the Articles hereof are for convenience only and do not define, limit or construe the contents of such Articles. Except as contemplated by the provisions of Article 18.4 and 19.9, nothing in this Agreement is intended, nor is deemed, to confer any rights or remedies upon any person not a party hereto. If applicable law shall impose a covenant of good faith and fair dealing in this Agreement, the parties hereto agree that such covenant shall not impose any rights or obligations that are inconsistent with a fair construction of the terms of this Agreement. Additionally, if applicable law shall impose such covenant, we and you acknowledge and agree that (a) this Agreement (and the relationship of the parties which arises from this Agreement) grants us the right to make decisions, take actions and/or refrain from taking actions not inconsistent with your express rights and obligations hereunder that may affect favorably or adversely your interests; (b) we will use our judgment in exercising such rights based on our assessment of our own interests and balancing those interests against the interests of the owners of **PLANET FITNESS** Businesses generally (including ourselves, and our Affiliates and other franchisees), and specifically without considering your individual interests or the individual interests of any other particular franchisee, and no court, arbitrator or judge or trier of fact, or any other person reviewing those activities or decisions may substitute their judgment for our judgment, in recognition of the fact that the long-term goals of a franchise system, and the long-term interests of both us and our franchisees taken together, require that we have the latitude to exercise our business judgment in administering, managing and overseeing the System; (c) we will have no liability to you for the exercise of our rights in this manner so long as such rights are not exercised in bad faith toward you; and (d) in the absence of such bad faith, no trier of fact in any legal action or arbitration proceeding shall substitute their judgment for our judgment so exercised.

19.16 **JOINT AND SEVERAL OWNERS' LIABILITY.** If two (2) or more persons are at any time the Owner of the BUSINESS hereunder, whether as partners or joint venturers, their obligations and liabilities to us will be joint and several.

19.17 **ANTI-TERRORISM LAWS.** You acknowledge that it is our intent to comply with all anti-terrorism laws enacted by the U.S. Government, including, but not limited to, the USA PATRIOT ACT or Executive Order 13324. You represent and warrant that neither you nor any of your Affiliates are now, nor have you or they ever been, a suspected terrorist or otherwise associated directly or indirectly with terrorist activity. You represent and warrant that to your actual and constructive knowledge that neither you, nor any of your Affiliates, or any funding source for the BUSINESS is now or during the term of this Agreement will be (1) identified on the sanctions or "blocked persons" lists at the United States Treasury's Office of Foreign Assets Control; (2) directly or indirectly owned or controlled by the government of any country that is subject to an embargo imposed by the United States government; (3) acting on behalf of the government of, or is involved in business arrangements or other transactions with, any country that is subject to such an embargo; (4) on the U.S. Department of Commerce Denied Persons, Entities and Unverified Lists, the U.S. Department of State's Debarred Lists, or on the U.S. Department of Treasury's Lists of Specialty Designated Nationals, Specialty Designated Narcotics Traffickers or Specialty Designated Terrorists, or any other lists of persons that are restricted or prohibited from doing business in the United States, as such lists may be amended from time to time (collectively, the "Lists"); or (5) selling products, goods, or services to, or otherwise enter into a business arrangement with, any person on any of the Lists or with which you are otherwise prohibited from doing business. You agree to notify us in writing immediately upon the occurrence of any act or event that would render

Exhibit 10W

any of these representations incorrect. At any time during the Term of this Agreement, if we are prohibited from doing business with you or any of your Affiliates under any anti-terrorism law enacted by the U.S. Government, then we may terminate this Agreement immediately.

19.18 **RIGHT TO INFORMATION.** You consent to us obtaining, using and disclosing to third parties (including, without limitation, financial institutions, legal and financial advisors, and existing or prospective franchisees), for any purpose we reasonably specify or as may be required by law, all financial and other information (including, without limitation, membership data and customer lists) contained in or resulting from information, data, materials, statements and reports related, directly or indirectly, to the BUSINESS. You acknowledge that our ability to obtain, use and disclose such information allows us to, among other things, better understand the performance of the System, continually improve the System, negotiate favorable arrangements with System suppliers, attract new franchisees, and assist existing franchisees in developing and operating their **PLANET FITNESS** Businesses.

19.19 **MULTIPLE COPIES AND ELECTRONIC RECORDS.** This Agreement may be executed in multiple copies, each of which will be deemed an original, and all of which when taken together shall constitute one and the same document. You consent and agree that: (i) we may provide and maintain all disclosures, agreements, amendments, notices, and all other evidence of transactions between us and you in electronic form, (ii) electronic copies of this Agreement and related agreements between us and you are valid, (iii) you will not contest the validity of the originals or copies of this Agreement and related agreements, absent proof of altered data or tampering, and (iv) this Agreement and related agreements may be executed by electronic means and such execution is legally binding and enforceable as an "electronic signature" and the legal equivalent of a handwritten signature.

19.20 **ENTIRE AGREEMENT BETWEEN THE PARTIES.** This Agreement together with any exhibits, addenda and appendices hereto constitute the sole agreement between you and us with respect to the entire subject matter of this Agreement and embody all prior agreements and negotiations with respect to your BUSINESS authorized hereunder. There are no representations or warranties of any kind, express or implied, except as contained herein or in the FDD provided to you in connection with this Agreement. You also acknowledge that your status as a **PLANET FITNESS** franchisee confers no right to be considered or preferred for any franchise or development opportunity except with respect to your rights in the Franchise expressly provided hereunder. You acknowledge that you received the FDD at least fourteen (14) days before you signed this agreement or any other agreement with us or an Affiliate or paid us or an Affiliate any money. Except to the extent we have negotiated changes to this Agreement that differ from the FDD, nothing in this Agreement is intended to disclaim representations that were provided to you in the FDD.

19.21 **AMENDMENTS.** Except with respect to address changes and updates to Appendix A as described herein, the terms of this Agreement may not be amended or modified unless such amendment or modification is (i) reduced to writing and signed by both you and us or (ii) both (a) approved, under the Voting Procedures, by at least seventy percent (70%) of all United States franchised **PLANET FITNESS** Businesses (excluding company-owned locations) and us and (b) applies equally to similarly situated franchisees. In such event, at our option you shall promptly sign an amendment to this Agreement reflecting such changes.

19.22 **AREA DEVELOPMENT AGREEMENT ADDENDUM.** This Article 19.22 is only applicable if you or your Affiliate have entered into an ADA with us, as referenced in Appendix F hereto. The ADA entered into with us contains certain negotiated provisions which are intended to apply to, and modify, future franchise agreements entered into between the parties. These negotiated provisions are set forth in Appendix F. Therefore, notwithstanding anything to the contrary set forth in this Agreement, to the extent any provision in Appendix F contradicts any provision in this Agreement, or is in addition to any provision of this Agreement, Appendix F shall control to the extent of such inconsistency or addition. Both we and you acknowledge and agree that Appendix F has been added at the request and for the convenience and benefit of all parties and with advice from their counsel.

Exhibit 10W

19.23 **TIME**. Time is of the essence to this Agreement.

20. **NOTICES AND PAYMENTS.** All written notices and reports permitted or required to be delivered by the provisions of this Agreement or the Operations Manual to us must be addressed to the General Counsel at the most current principal business address of which you have been notified. All payments will be deemed delivered when received and will be deemed delivered by EFT or bank-wire transfer upon telephone or electronic confirmation with the receiving bank. All written notices and reports permitted or required to be delivered by the provisions of this Agreement to you shall be addressed to your Responsible Owner or Approved Operator at your most current principal business address of which we have been notified, or the mailing address listed for your Responsible Owner or Approved Operator as listed on Appendix A. We may deliver copies of notices hereunder to your Owners, landlord, lenders or other parties that have a right to receive copies thereof. We will exercise reasonable efforts to promptly notify you of any copies of notices delivered to third parties. Notices or reports will be deemed delivered:

(1) at the time delivered by hand;

(2) one (1) Business Day after transmission by e-mail or other electronic system, provided there is evidence of delivery and notice is also promptly provided pursuant to the methods set forth in subsections (1), (3), or (4);

(3) one (1) Business Day after being placed in the hands of a commercial courier service for next Business Day delivery, provided there is evidence of delivery; or

(4) five (5) Business Days after placement in the United States Mail by Registered or Certified Mail, Return Receipt Requested, postage prepaid.

[Remainder of page intentionally left blank; signatures to follow]

Exhibit 10W

IN WITNESS WHEREOF, the parties hereto have executed and delivered this Agreement as of the Effective Date.

PLANET FITNESS FRANCHISING LLC

By: ____

Print Name: Justin Vartanian

Title: General Counsel and SVP, International Division

EFFECTIVE DATE: ________________________

EACH OF THE UNDERSIGNED PARTIES REPRESENTS AND WARRANTS THAT SUCH PARTY HAS NOT RELIED UPON ANY GUARANTEES CONCERNING REVENUE, PROFIT OR THE SUCCESS OF THIS FRANCHISE IN SO SIGNING. FRANCHISEE ACKNOWLEDGES AND AGREES THAT IT (1) HAS SPECIFICALLY REVIEWED THE COMPLETED VERSION OF APPENDICES A (OWNERSHIP ADDENDUM), D (SILENT INVESTORS), AND F (AREA DEVELOPMENT AGREEMENT ADDENDUM), (2) IS BOUND THEREBY, (3) IS BEST POSITIONED, BETWEEN THE PARTIES, TO VERIFY THE ACCURACY OF THE INFORMATION PROVIDED AND CONTAINED THEREIN AND (4) HAS CAUSED ALL REQUIRED PARTIES TO RECEIVE, REVIEW AND EXECUTE APPENDIX C (PERSONAL COVENANTS REGARDING CONFIDENTIALITY AND NON-COMPETITION). AS SUCH, WE ARE ENTITLED TO RELY ON SUCH INFORMATION. FRANCHISEE REPRESENTS AND WARRANTS THAT ALL SUCH INFORMATION IS TRUE, CORRECT AND COMPLETE AS OF THE DATE OF FRANCHISEE'S EXECUTION OF THIS AGREEMENT, PROVIDED, HOWEVER, THAT AN IMMATERIAL INACCURACY IN SUCH INFORMATION SHALL NOT BE A DEFAULT UNDER THIS AGREEMENT.

BY SIGNING BELOW, I REPRESENT AND WARRANT THAT I HAVE HAD AMPLE TIME TO REVIEW AND DISCUSS THIS AGREEMENT WITH MY ATTORNEY(S). I UNDERSTAND THAT THIS AGREEMENT GOVERNS OUR BUSINESS RELATIONSHIP WITH RESPECT TO THE BUSINESS.

[FRANCHISEE]

By: ____
(Authorized Representative)

Print Name:__________________________________

Title: ______________________________________

Dated: _____________________________________

Exhibit 10W

APPENDIX A
TO THE FRANCHISE AGREEMENT

OWNERSHIP ADDENDUM

1. **RESPONSIBLE OWNER.** The name, e-mail address, and address of the Responsible Owner is as follows: [Name (Email), Address, City, State, Postal].

2. **APPROVED OPERATOR.** The name, e-mail address, and address of the Approved Operator is as follows: [Name (Email), Address, City, State, Postal].

3. **ENTITY DETAILS.**

Franchisee was organized as a [limited liability company/corporation] on ____________________, under the laws of the [State/Commonwealth] of ______________________. Its Federal Identification Number is ___________________. It has not conducted business under any name other than its corporate or company name. Its principal business address is ____.

4. **OWNERS.**

You represent and warrant that the following is a complete and accurate list of all Owners of any direct or indirect ownership interest whatsoever in you, including the full name, email address, and mailing address of each Owner, and fully describes the nature and extent of each Owner's interest in you. You represent and warrant that each Owner is the sole and exclusive legal and beneficial owner of such Owner's ownership interest in you, free and clear of all liens, restrictions, agreements and encumbrances of any kind or nature, other than those required or permitted by this Agreement. If this Franchise Agreement is entered into pursuant to an ADA, your ownership shall be the same as set forth in the ADA, unless otherwise noted below.

Owner's Name and Contact Information	Percentage and Nature of Ownership Interest
____	____
____	____
____	____

[Remainder of page intentionally left blank; end of Appendix A]

Exhibit 10W

APPENDIX B
TO FRANCHISE AGREEMENT

GUARANTY OF FRANCHISEE'S OBLIGATIONS ("Guaranty")

In consideration of, and as an inducement to, the execution of the Franchise Agreement dated as of the Effective Date, (the "Agreement") by and between Planet Fitness Franchising LLC ("Franchisor"), and _________________________ ("Franchisee") each of the undersigned Affiliate(s) or Owners of Franchisee hereby unconditionally: (1) guarantees to Franchisor and its successors and assigns, for the term of the Agreement and thereafter as provided in the Agreement, that Franchisee shall punctually pay and perform each and every undertaking, agreement and covenant of Franchisee set forth in the Agreement (and any amendments) and that each and every representation of Franchisee made in connection with the Agreement (and any amendments) are true, correct and complete in all respects at and as of the time given; and (2) agree to be bound by, and liable for the breach of, each and every provision in the Agreement (and any amendments) binding on Franchisee, including, without limitation, the confidentiality obligations and non-competition covenants in Articles 8 and 16 of the Agreement, respectively.

Each of the undersigned waives: (a) acceptance and notice of acceptance by Franchisor of the foregoing undertakings; (b) notice of demand for payment of any indebtedness or nonperformance of any obligations hereby guaranteed; (c) protest and notice of default to any party with respect to the indebtedness or nonperformance of any obligations hereby guaranteed; (d) any right the undersigned may have to require that an action be brought against Franchisee or any other person as a condition of liability; (e) notice of any amendment to the Agreement; and (f) any and all other notices and legal or equitable defenses to which the undersigned may be entitled.

Each of the undersigned consents and agrees that: (i) the undersigned's direct and immediate liability under this guaranty shall be joint and several in each and every respect; (ii) the undersigned shall render any payment or performance required under the Agreement upon demand if Franchisee fails or refuses to do so punctually; (iii) such liability shall not be contingent or conditioned upon pursuit by Franchisor of any remedies against Franchisee or any other person; and (iv) such liability shall not be diminished, relieved or otherwise effected by any extension of time, credit or other indulgence which the Franchisor may from time to time grant to Franchisee or to any other person including, without limitation, the acceptance of any partial payment or performance or the compromise or release of any claims, none of which shall in any way modify or amend this guaranty, which shall be continuing and irrevocable until satisfied in full.

It is further understood and agreed by the undersigned that the provisions, covenants and conditions of the Guaranty will inure to the benefit of our successors and assigns.

This Guaranty shall be governed by the governing law provisions set forth in Article 19.10 of the Agreement and all disputes related to it shall be resolved in accordance with the dispute resolution provisions set forth in Articles 19.9, 19.11, and 19.12 of the Agreement.

If any Guarantors are natural persons, such Guarantors agree to be personally bound and personally liable under this Guaranty.

If any Guarantors are Entities, such Guarantors represent and warrant that they are duly formed and in good standing in the jurisdiction in which they are organized; and shall promptly provide to Franchisor their organizational documents, shall, upon request by Franchisor, provide their balance sheet and statement of income on an annual basis by March 30 of each year; and shall promptly provide to Franchisor any information regarding any transfers of interest or sale of substantial assets in the undersigned. In the event of a transfer of control of a Guarantor that is an Entity or the impairment of the financial capacity of a Guarantor that is an Entity, in Franchisor's reasonable judgment, Franchisor shall have the right to require a personal guaranty from Franchisee's Owners in substantially the same form as in this Guaranty.

No default or failure to comply with the terms of this Guaranty shall constitute a default of any other franchise agreement that the undersigned may have with Franchisor.

Exhibit 10W

IN WITNESS WHEREOF, each of the undersigned has hereunto affixed the undersigned's signature, under seal, as of the Effective Date of the Agreement.

GUARANTOR(S):

____
(Signature)

____
(Print Name)

____
(Signature)

____
(Print Name)

[AFFILIATE ENTITY]

By: ___________________________________
(Authorized Representative)

Print Name:_____________________________

Title: _________________________________

Dated: ________________________________

[Remainder of page intentionally left blank; end of Appendix B]

Exhibit 10X

PLANET FITNESS®

EXHIBIT "B"
TO THE DISCLOSURE DOCUMENT

NONDISCLOSURE & NON-USE AGREEMENT

Exhibit 10X

CONFIDENTIALITY AND NONDISCLOSURE AGREEMENT

1. In connection with the Purpose defined herein, you ("Receiving Party") will be provided with or learn certain non-public, confidential and/or proprietary information (the "Confidential Information", as further defined herein) belonging to Planet Fitness Franchising LLC and/or its parents, subsidiaries and affiliated entities (collectively, with their respective employees, officers, directors, managers, and members, "Planet Fitness"). By executing this Confidentiality and Nondisclosure Agreement (this "Agreement") you agree to abide by and be subject to its terms with regard to your use of all such Confidential Information.

2. As used herein, "Confidential Information" shall mean all information disclosed by or on behalf of Planet Fitness (including that of all subsidiaries and affiliates) including, without limitation, Planet Fitness' lists and other data, business volumes or usage, financial information and analyses, fee structure and other pricing information, information related to software, software documentation, manuals, formulas, trade secrets, security procedures, information concerning business plans or business strategy, presentations, proposals, and any and all information about Planet Fitness' customers and their affairs and all information received by Planet Fitness from any third party with any understanding, express or implied, that the information would not be disclosed, whether written or in machine-readable form, or disclosed orally or visually to Receiving Party, as well as all analyses, compilations, studies or other documents prepared by or at the direction of Receiving Party which contain or otherwise reflect such information. Confidential Information also includes (a) the existence of this Agreement and the fact that Confidential Information has been disclosed, (b) that you are or may be providing services to Planet Fitness in connection with the Purpose (as defined herein) or (c) any terms, conditions or other facts with respect to the Purpose, including the status thereof. Information will be deemed not to be Confidential Information if it (i) is already in your possession separate and apart from disclosure by Planet Fitness, (ii) becomes generally available in the public domain other than as a result of unauthorized disclosure by any person, or (iii) is acquired on a non-confidential basis from a third party not in breach of an obligation of secrecy to Planet Fitness.

3. By executing this Agreement, you agree to use the Confidential Information only for the purpose of evaluating a potential business relationship with Planet Fitness (the "Purpose") and not to disclose any Confidential Information to any person or entity except (i) to those of your directors, officers, managers, and employees necessary to accomplish the Purpose, or (ii) to others only with the prior written consent of Planet Fitness. You agree that prior to your disclosure of any Confidential Information to any person(s) permitted to receive it, you will inform such person(s) of the confidential nature of the Confidential Information and require such person(s) to agree to be bound by the terms of this Agreement as if a party hereto. You shall be responsible for any failure to comply with the terms of this Agreement by any person or entity to whom you disclose Confidential Information, and you must take all commercially reasonable measures to restrain all parties to whom you have disclosed Confidential Information from unauthorized disclosure or use of any Confidential Information. You must take all commercially reasonable measures to protect the Confidential Information from unauthorized access.

4. In the event that you or any person to whom you have disclosed Confidential Information become legally compelled by a judicial or legislative order of a governmental authority or court of competent jurisdiction to disclose any of the Confidential Information, you shall provide Planet Fitness with prompt prior written notice of such requirement so that Planet Fitness may seek a protective order or other appropriate remedy and/or waive compliance with the terms of this Agreement and, upon Planet Fitness request, you shall take all reasonable steps requested to assist Planet Fitness in contesting such request for disclosure. In the event that such protective order or other remedy is not obtained, or that Planet Fitness waives compliance with the provisions hereof, you agree to furnish only that portion of the Confidential Information which you are advised by counsel is legally required and to exercise commercially reasonable efforts to obtain assurance that confidential treatment will be accorded such Confidential Information.

5. You understand and acknowledge that Planet Fitness is not making any representation or warranty, express or implied, as to the accuracy or completeness of the Confidential Information and shall have no liability to you or any other person resulting from your use of the Confidential Information.

6. All Confidential Information, and any Derivatives (defined below) thereof, whether created by Planet Fitness or Receiving Party, shall be the property of Planet Fitness and no license or other rights to Confidential Information or Derivatives is granted or implied hereby. For purposes of this Agreement, "Derivatives" shall mean: (a) for copyrightable or copyrighted material, any translation, abridgment, revision or other form in which existing Confidential Information may be recast, transformed or adapted; (b) for patentable or patented Confidential Information, any improvement thereon; and (c) for Confidential Information protected by trade secret, any new material derived from such existing trade secret Confidential Information. Receiving Party hereby does and will assign to Planet Fitness all of Receiving Party's rights, title in interest and interest in and to the Derivatives.

7. In the event of your breach (either actual or threatened) of this Agreement, you agree that Planet Fitness shall be entitled to any and all remedies available, including injunctive and other equitable relief (without necessity of posting any bond or other security or proving special damages), and that you shall not oppose the grant of such relief. You further agree that you will indemnify, defend and hold harmless Planet Fitness with respect to any and all losses, damages, claims, costs and expenses resulting or arising from any failure by you or any party to whom you disclose Confidential Information to comply with the terms of this Agreement.

8. Receiving Party may only make such copies of written, recorded, or machine-readable Confidential Information as are necessary to accomplish the Purpose. All such Confidential Information, and all copies thereof, shall be held under the terms and provisions of this Agreement. Receiving Party agrees that, upon Planet Fitness' written request, Receiving Party shall promptly (and in no event later than 14 days thereafter) destroy or return to Planet Fitness all Confidential Information; provided, that Receiving Party may retain, in a secure location, a copy of such documents and records for purposes of defending any legal proceeding or as is required to be maintained in order to satisfy any law, rule, or regulation to which Receiving Party is subject. Destruction of materials will be confirmed by Receiving Party to Planet Fitness in writing. Notwithstanding the return or destruction of any Confidential Information, Receiving Party will continue to hold in confidence the contents of all Confidential Information, including, without limitation, any oral Confidential Information.

9. The Receiving Party acknowledges that it is aware that the Confidential Information may relate to publicly traded securities. The Receiving Party is aware of the restrictions imposed by applicable securities laws restricting trading in securities while in possession of material non-public information and on communication of such information when it is reasonably foreseeable that the recipient is likely to trade such securities, in reliance on such information. The Receiving Party agrees not to trade, either directly or through other persons or entities based on the Confidential Information in a manner that would violate the securities law of any applicable jurisdiction, including, without limitation, the United States securities laws.

10. Until five (5) years from the Effective Date of this Agreement (the "Confidentiality Period"), the Receiving Party shall hold in trust and confidence any and all Confidential Information received by it hereunder and shall not disclose such Confidential Information to anyone except pursuant to Section 3 above. During the Confidentiality Period and thereafter, the Receiving Party shall not use the Confidential Information for any purpose, except in connection with the Purpose or as otherwise specified in a separate written instrument executed by the parties hereto. Upon entry by the parties into a definitive franchise agreement or area development agreement, any Confidential Information disclosed under this Agreement shall also be deemed "Confidential Information" under the applicable definitive agreement.

11. It is further understood and agreed that no failure or delay by Planet Fitness in exercising any right, power or privilege hereunder will operate as a waiver thereof, nor will any single or partial exercise thereof preclude any other or further exercise thereof or the exercise of any right, power or privilege hereunder. If any provision of this Agreement is found to be invalid, the remaining provisions shall remain fully in effect.

12. This Agreement does not supersede or modify any prior written agreements previously entered into by and between the parties, and does not relieve the parties of their respective obligations under such prior agreements.

13. This Agreement is for the sole benefit of Planet Fitness, may be enforced directly by Planet Fitness, and shall be governed by and construed in accordance with the laws of the State of New Hampshire, regardless of the laws that might otherwise govern under applicable principles of conflicts of law thereof. The sole and exclusive venue for any dispute or claim arising from this Agreement shall be the courts of the State of New Hampshire.

Exhibit 10X

A t an a r t y t R n Party a t E t
Dat t rt :

Receiving Party: ____

Signature:____

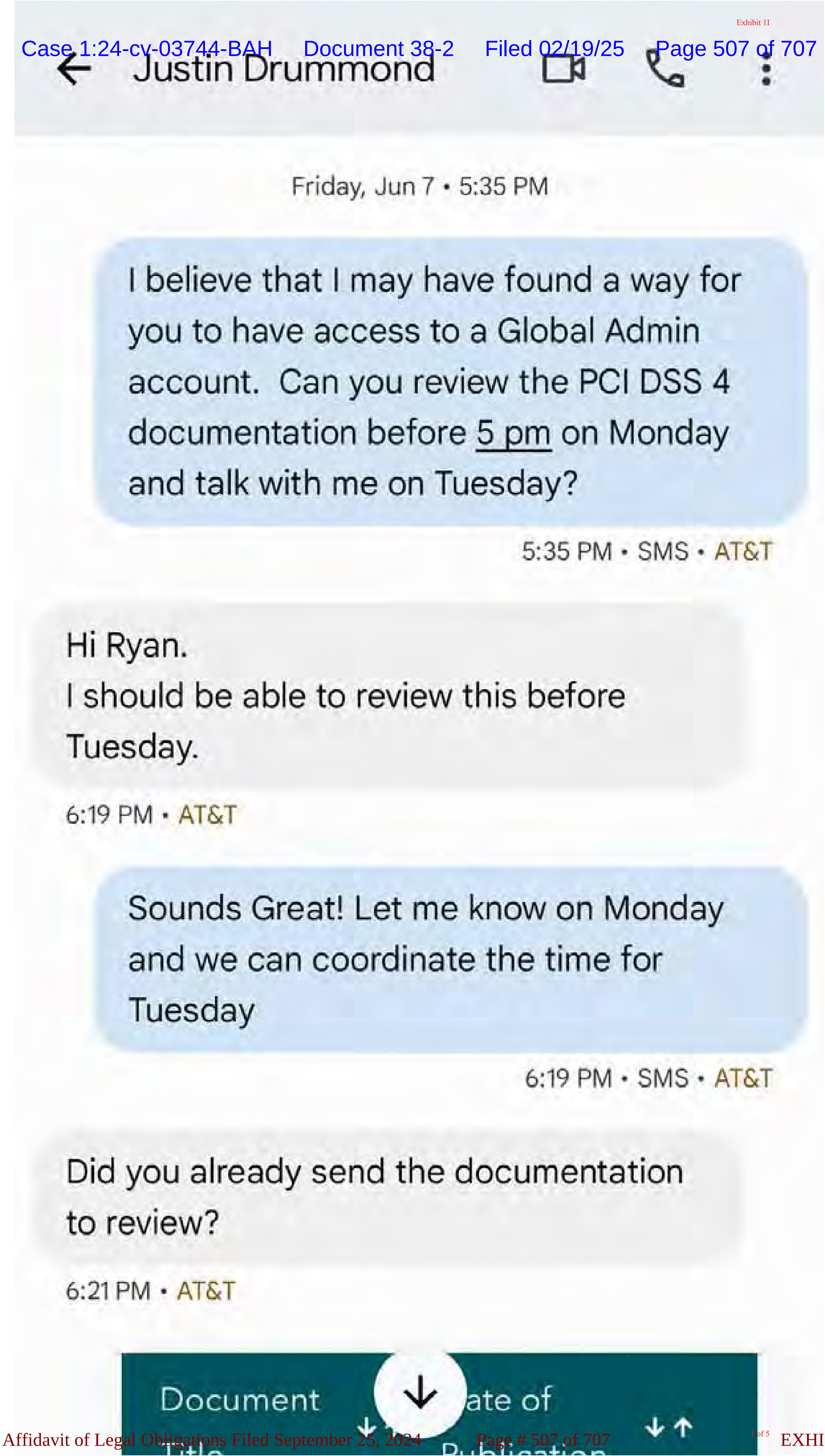
Print Name: ____

Address: ____

____

E t Dat : ____

Signature page to the Planet Fitness Confidentiality and Nondisclosure Agreement



Justin Drummond

Friday, Jun 7 • 5:35 PM

I believe that I may have found a way for you to have access to a Global Admin account. Can you review the PCI DSS 4 documentation before 5 pm on Monday and talk with me on Tuesday?

5:35 PM • SMS • AT&T

Hi Ryan.
I should be able to review this before Tuesday.

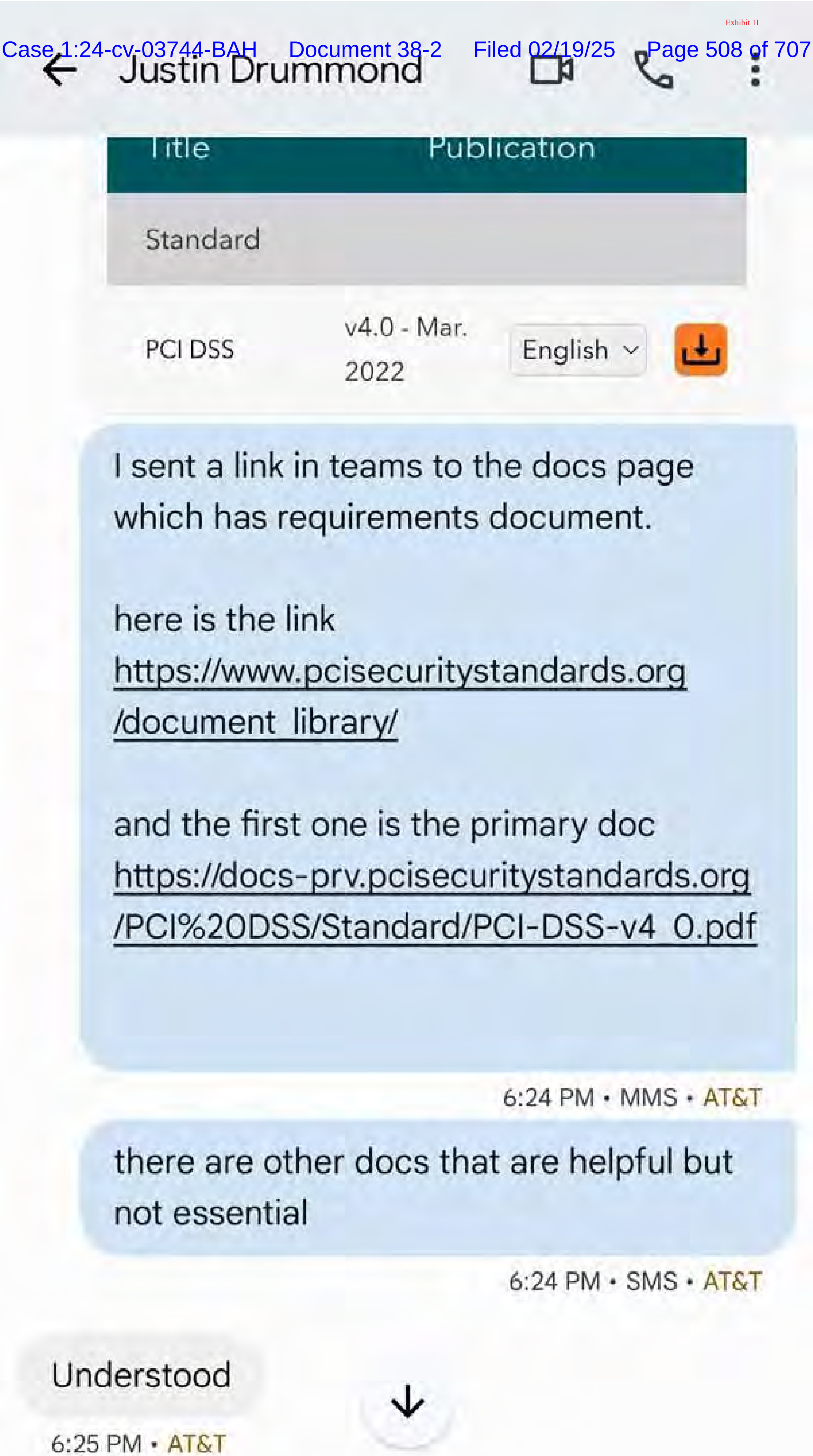
6:19 PM • AT&T

Sounds Great! Let me know on Monday and we can coordinate the time for Tuesday

6:19 PM • SMS • AT&T

Did you already send the documentation to review?

6:21 PM • AT&T



Title	Publication	
Standard		
PCI DSS	v4.0 - Mar. 2022	English

I sent a link in teams to the docs page which has requirements document.

here is the link
https://www.pcisecuritystandards.org/document_library/

and the first one is the primary doc
https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf

6:24 PM • MMS • AT&T

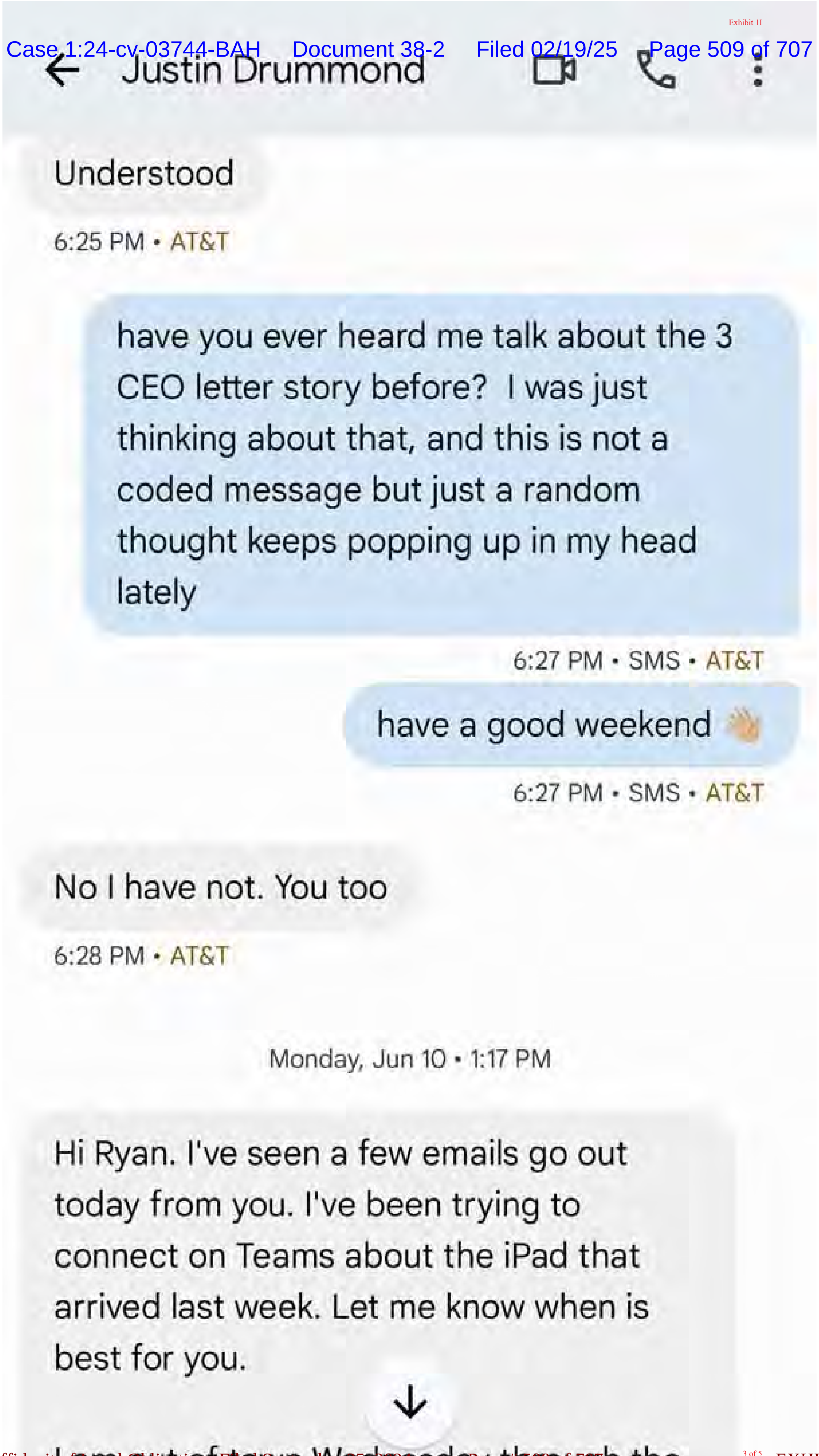
there are other docs that are helpful but not essential

6:24 PM • SMS • AT&T

Understood

6:25 PM • AT&T

Exhibit II



Justin Drummond

Understood

6:25 PM • AT&T

have you ever heard me talk about the 3 CEO letter story before? I was just thinking about that, and this is not a coded message but just a random thought keeps popping up in my head lately

6:27 PM • SMS • AT&T

have a good weekend 👋

6:27 PM • SMS • AT&T

No I have not. You too

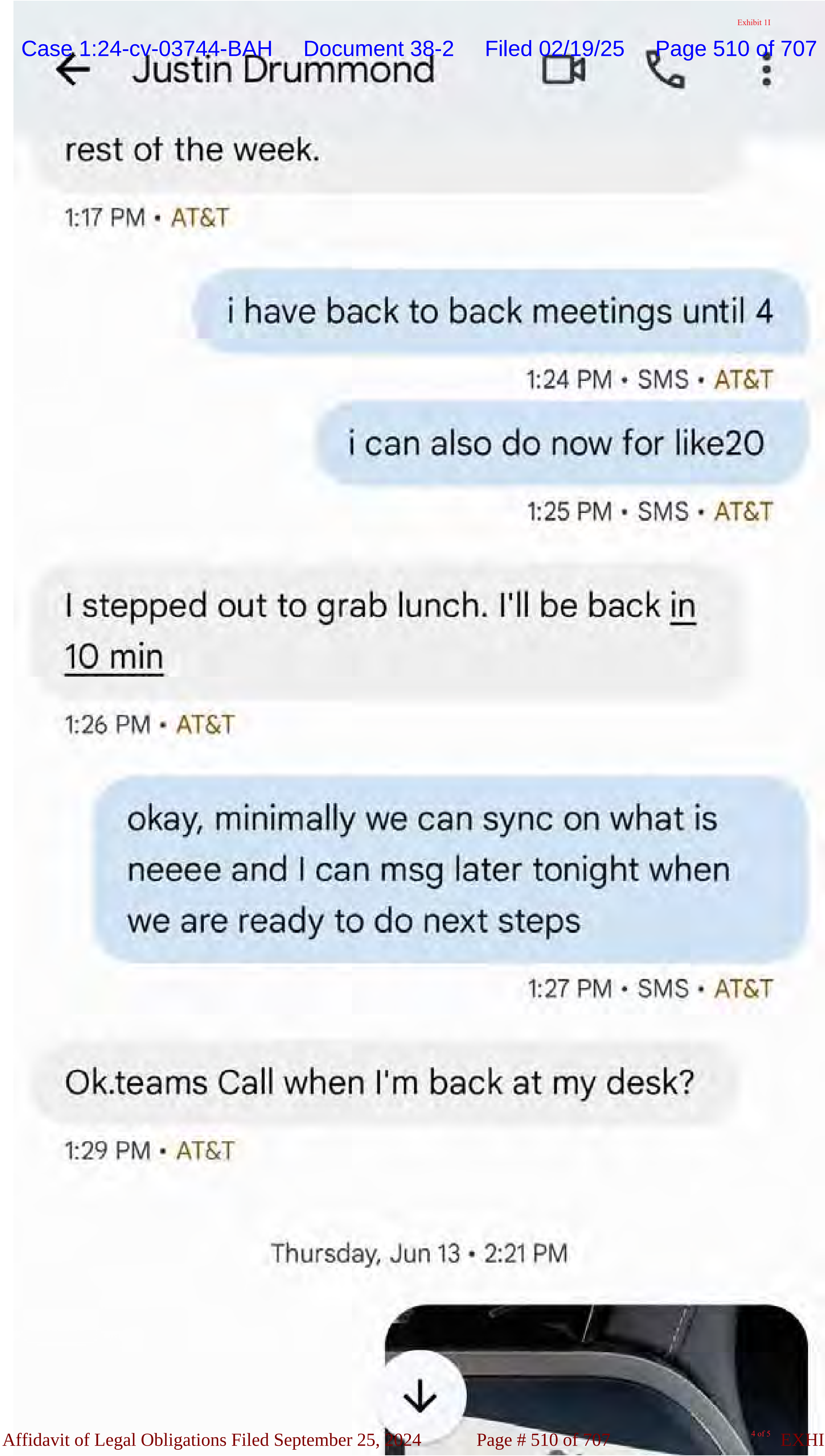
6:28 PM • AT&T

Monday, Jun 10 • 1:17 PM

Hi Ryan. I've seen a few emails go out today from you. I've been trying to connect on Teams about the iPad that arrived last week. Let me know when is best for you.

I am out of town Wednesday through the

Exhibit 11



rest of the week.

1:17 PM • AT&T

i have back to back meetings until 4

1:24 PM • SMS • AT&T

i can also do now for like20

1:25 PM • SMS • AT&T

I stepped out to grab lunch. I'll be back in 10 min

1:26 PM • AT&T

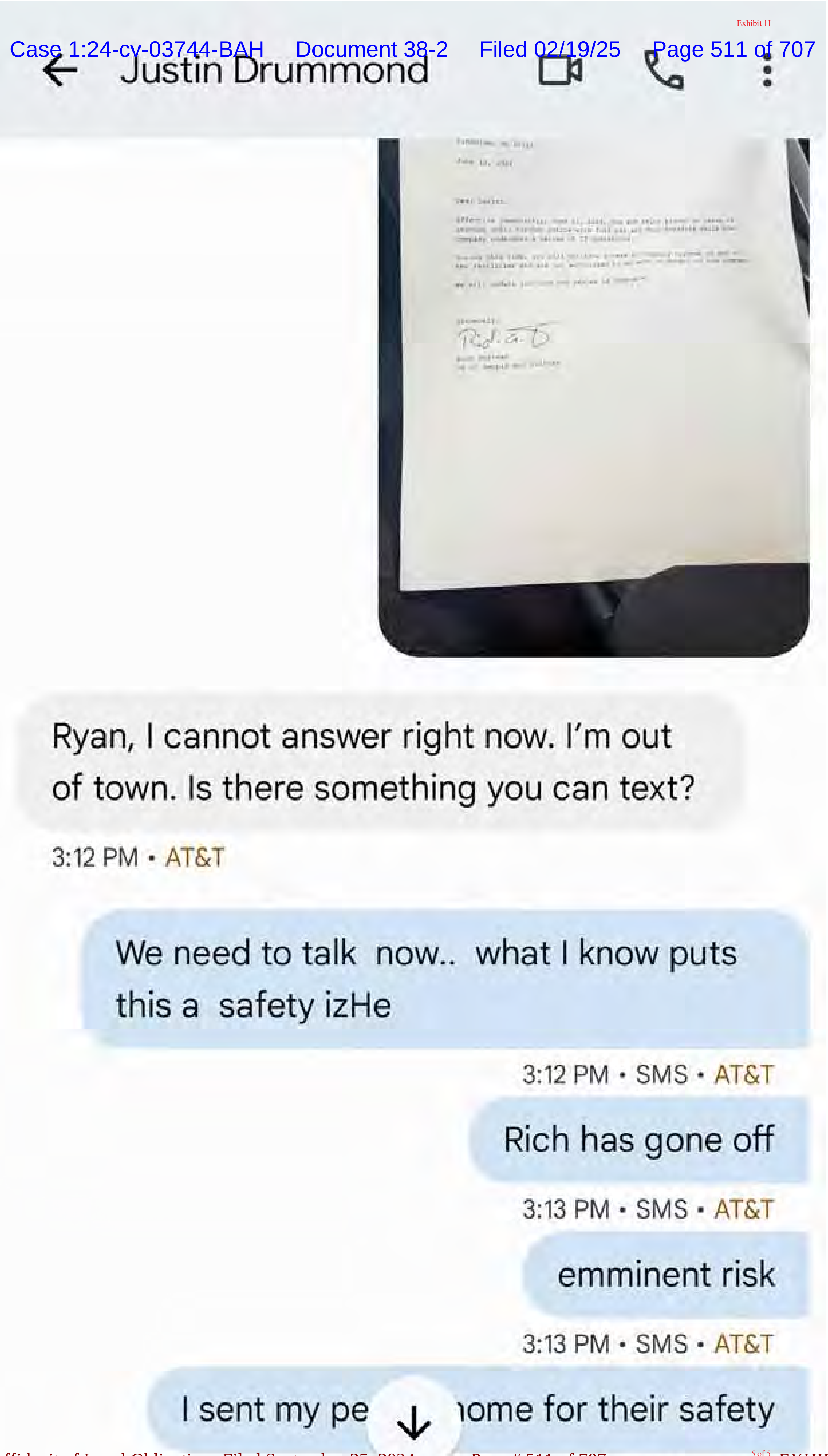
okay, minimally we can sync on what is neeee and I can msg later tonight when we are ready to do next steps

1:27 PM • SMS • AT&T

Ok.teams Call when I'm back at my desk?

1:29 PM • AT&T

Thursday, Jun 13 • 2:21 PM



[illegible]

Ryan, I cannot answer right now. I'm out of town. Is there something you can text?

3:12 PM • AT&T

We need to talk now.. what I know puts this a safety izHe

3:12 PM • SMS • AT&T

Rich has gone off

3:13 PM • SMS • AT&T

emminent risk

3:13 PM • SMS • AT&T

I sent my pe ↓ ıome for their safety

3:13 PM • SMS • AT&T

Exhibit 1T

Ryan Wagner <ryan@mxt3.com>

Urgent FROM ryan.wagner@ohanagp.com

1 message

Ryan Wagner <ryan@mxt3.com> Fri, May 24, 2024 at 9:27 PM
Reply-To: ryan@mxt3.com
To: geoff.vanmaastricht@pfhq.com

As a precautionary measure, I have created you an account as a Global Admin with other roles you will need to manage our environment.

Geoff.PFHQ@ohanagp.com

My number is 703-303-1113

This is my personal email. I can send/receive communications on both emails.

Exhibit 1T

Ryan Dillon-Capps

From:	Rolando Pedraza <rpedraza@cieloit.com>
Sent:	Thursday, June 6, 2024 5:04 PM
To:	Ryan Wagner
Cc:	Shannon Anderson; Dante Martinez
Subject:	Re: PCI DSS 4 Compliance + Best Practices

CAUTION: This email originated from outside the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Hello Ryan,

First, thank you for sharing all the changes happening in Ohana to enhance security.

I'm aware that Brooks is no longer with Ohana, and I understand the general idea of what you would like to accomplish with me taking on the Global Admin role. However, I would like to have a call with you next week to understand better what it entails and to align our ideas more closely.

What I can say for sure is that this is something Cielo can definitely help you with; I just need to understand better how to achieve the results you're expecting.

Could you please let me know a convenient time for the call next week?

Thanks,

Rolando Pedraza Director of Delivery Operations

CieloIT
IT's in the Cloud™

T: 806.503.2181 x 101
C: 806.705.7149
E: rpedraza@cieloit.com
W: www.cieloit.com

Confidentiality Notice: This message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure, or distribution is strictly prohibited. If you are not the intended recipient, please contact the sender by reply e-mail and destroy all copies of the original message.

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Thursday, June 6, 2024 6:00
To: Rolando Pedraza <rpedraza@cieloit.com>
Cc: Shannon Anderson <sanderson@cieloit.com>; Dante Martinez <dante.martinez@ohanagp.com>
Subject: PCI DSS 4 Compliance + Best Practices

@Rolando Pedraza You may already be aware that we have recently implemented several changes to align with PCI DSS 4 and best practices. These changes include:

- Separating Global Administrator accounts from accounts used for daily tasks

Exhibit 1T

- Implementing Emergency Break Glass accounts
- Aligning with least privilege-based assignments

With Baltimore Consulting and Ryan Brooks no longer with us, we need another person to manage a Global Administrator account. Given your position as Director of Managed Services, I believe you are an ideal candidate. If you and Shannon agree, here are the requirements for this role:

1. **FIDO 2 Security Key**: We recommend the Thetis Pro FIDO2 Security Key, priced at $29.99. You can purchase it yourself, through Cielo, or we can make arrangements. Thetis Pro FIDO2 Security Key, Two-Factor Authentication NFC Security Key, Dual USB Ports Type A & Type C for Multi-Factor Protection (HOTP)

2. **Familiarity with PCI DSS 4**: PCI DSS 4 Documentation. We should schedule a time to review the impact of PCI DSS 4 on our operations. The new version has expanded the scope and added flexibility, which can be challenging.

3. **Microsoft Best Practices**: The changes in PCI DSS 4 align with current best practices. We need to prepare for several mandatory changes that Microsoft will impose over the next 15 months.

    - Microsoft Best Practices
    - Security Planning
    - Emergency Access Accounts
    - Separation of Global Admin Accounts

Maintaining PCI compliance is crucial because all Planet Fitness locations share the same processor and compliance requirements. A violation by one group affects the entire organization.

Additionally, ensuring redundancy is essential to maintain security and PCI compliance during an unforeseen event. Currently, all Ohana IT operations and our emergency account keys are based in Maryland, which poses a potential issue in the event of a regional disaster. Your geographical location allows us to ensure regional redundancy.

This message may include text created with the help of natural language processing.

Book time to meet with me

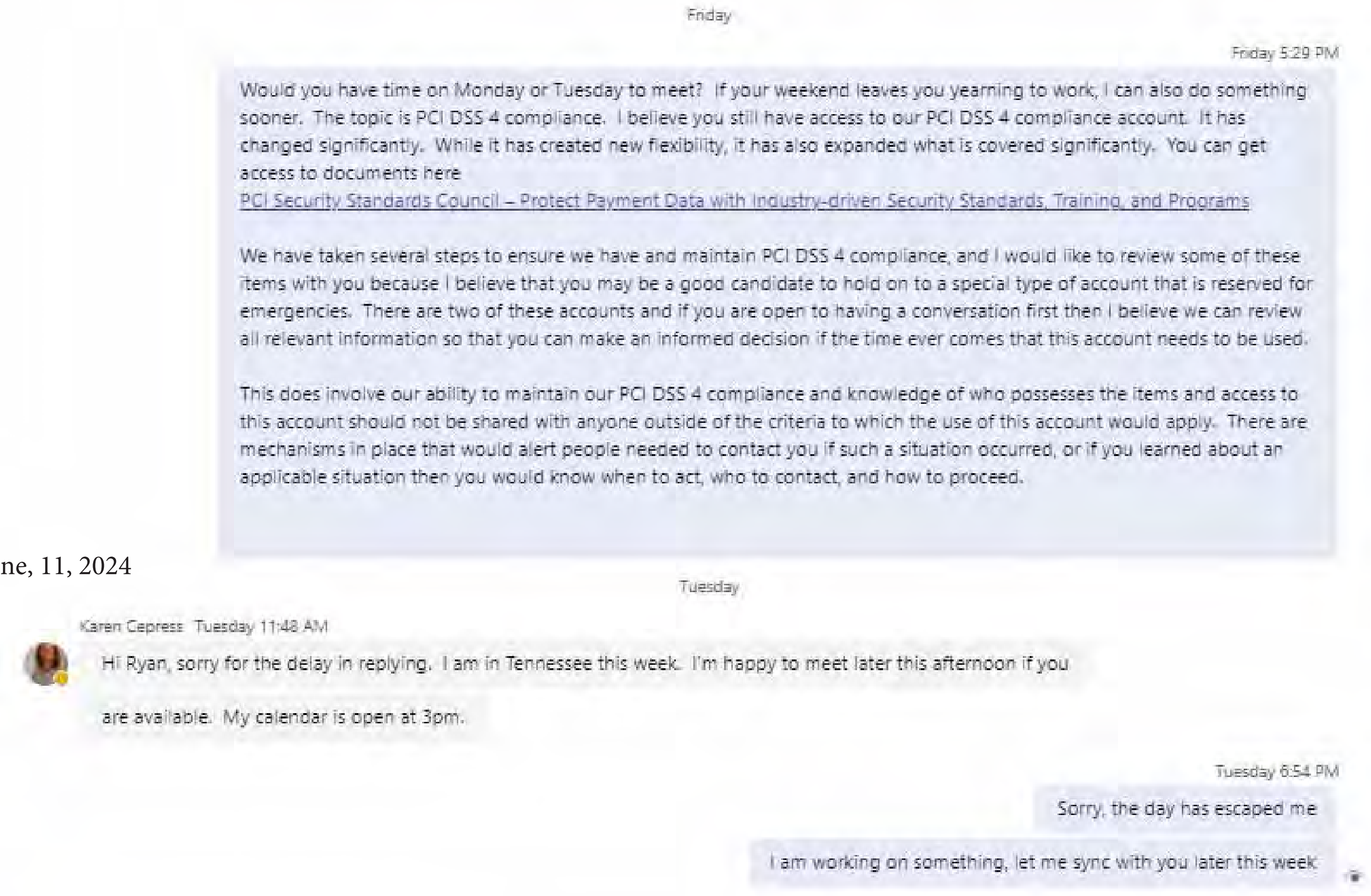
Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

Exhibit 1T

Friday June 7, 2024



Friday 5:29 PM

Would you have time on Monday or Tuesday to meet? If your weekend leaves you yearning to work, I can also do something sooner. The topic is PCI DSS 4 compliance. I believe you still have access to our PCI DSS 4 compliance account. It has changed significantly. While it has created new flexibility, it has also expanded what is covered significantly. You can get access to documents here
PCI Security Standards Council – Protect Payment Data with Industry-driven Security Standards, Training, and Programs

We have taken several steps to ensure we have and maintain PCI DSS 4 compliance, and I would like to review some of these items with you because I believe that you may be a good candidate to hold on to a special type of account that is reserved for emergencies. There are two of these accounts and if you are open to having a conversation first then I believe we can review all relevant information so that you can make an informed decision if the time ever comes that this account needs to be used.

This does involve our ability to maintain our PCI DSS 4 compliance and knowledge of who possesses the items and access to this account should not be shared with anyone outside of the criteria to which the use of this account would apply. There are mechanisms in place that would alert people needed to contact you if such a situation occurred, or if you learned about an applicable situation then you would know when to act, who to contact, and how to proceed.

Tuesday June, 11, 2024

Karen Cepress Tuesday 11:48 AM

Hi Ryan, sorry for the delay in replying. I am in Tennessee this week. I'm happy to meet later this afternoon if you

are available. My calendar is open at 3pm.

Tuesday 6:54 PM

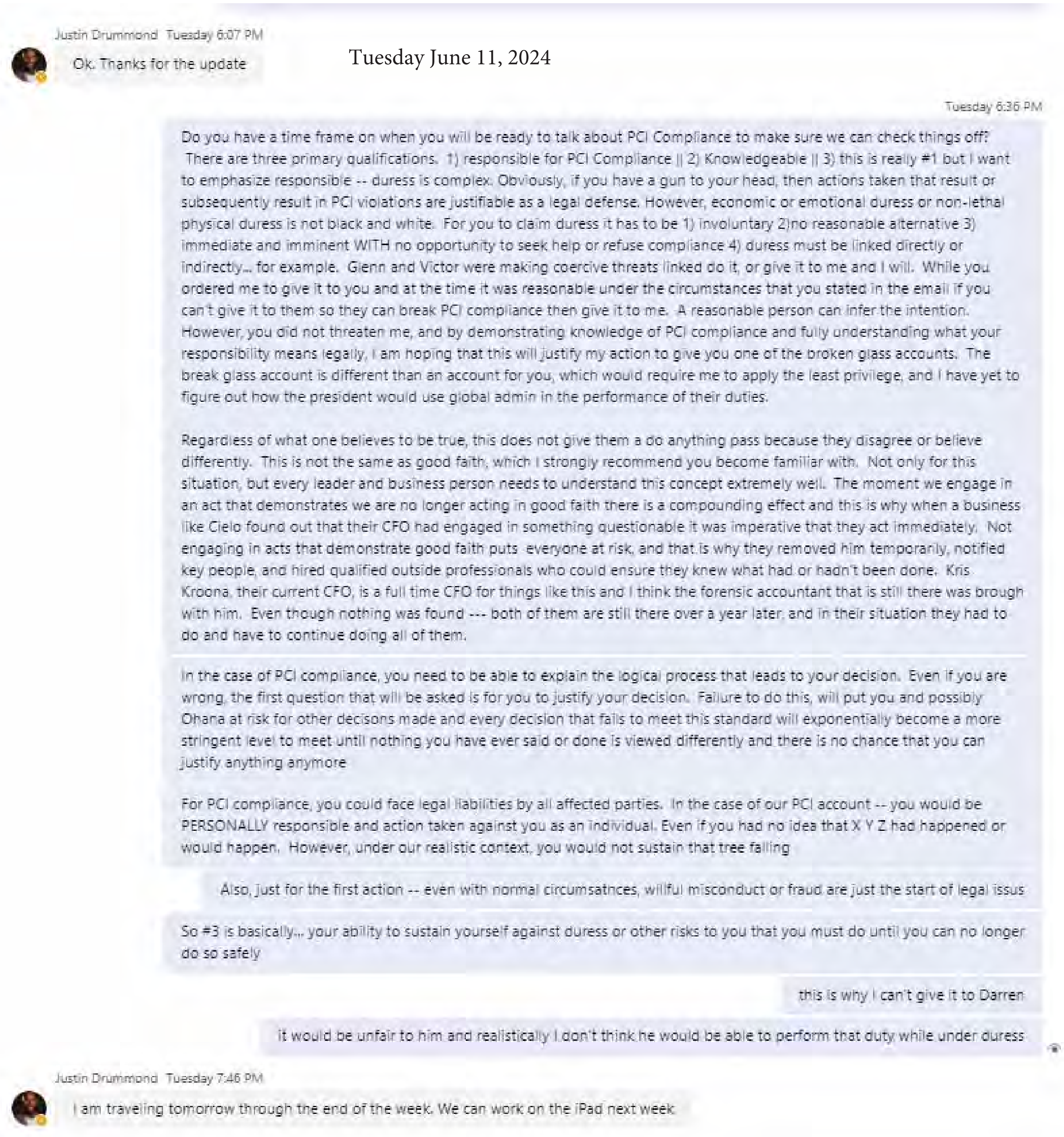
Sorry, the day has escaped me

I am working on something, let me sync with you later this week

4 of 5

Exhibit 1T

5 of 5



Justin Drummond Tuesday 6:07 PM

Ok. Thanks for the update

Tuesday June 11, 2024

Tuesday 6:36 PM

Do you have a time frame on when you will be ready to talk about PCI Compliance to make sure we can check things off? There are three primary qualifications. 1) responsible for PCI Compliance || 2) Knowledgeable || 3) this is really #1 but I want to emphasize responsible -- duress is complex. Obviously, if you have a gun to your head, then actions taken that result or subsequently result in PCI violations are justifiable as a legal defense. However, economic or emotional duress or non-lethal physical duress is not black and white. For you to claim duress it has to be 1) involuntary 2)no reasonable alternative 3) immediate and imminent WITH no opportunity to seek help or refuse compliance 4) duress must be linked directly or indirectly... for example. Glenn and Victor were making coercive threats linked do it, or give it to me and I will. While you ordered me to give it to you and at the time it was reasonable under the circumstances that you stated in the email if you can't give it to them so they can break PCI compliance then give it to me. A reasonable person can infer the intention. However, you did not threaten me, and by demonstrating knowledge of PCI compliance and fully understanding what your responsibility means legally, I am hoping that this will justify my action to give you one of the broken glass accounts. The break glass account is different than an account for you, which would require me to apply the least privilege, and I have yet to figure out how the president would use global admin in the performance of their duties.

Regardless of what one believes to be true, this does not give them a do anything pass because they disagree or believe differently. This is not the same as good faith, which I strongly recommend you become familiar with. Not only for this situation, but every leader and business person needs to understand this concept extremely well. The moment we engage in an act that demonstrates we are no longer acting in good faith there is a compounding effect and this is why when a business like Cielo found out that their CFO had engaged in something questionable it was imperative that they act immediately. Not engaging in acts that demonstrate good faith puts everyone at risk, and that is why they removed him temporarily, notified key people, and hired qualified outside professionals who could ensure they knew what had or hadn't been done. Kris Kroona, their current CFO, is a full time CFO for things like this and I think the forensic accountant that is still there was brough with him. Even though nothing was found --- both of them are still there over a year later, and in their situation they had to do and have to continue doing all of them.

In the case of PCI compliance, you need to be able to explain the logical process that leads to your decision. Even if you are wrong, the first question that will be asked is for you to justify your decision. Failure to do this, will put you and possibly Ohana at risk for other decisons made and every decision that fails to meet this standard will exponentially become a more stringent level to meet until nothing you have ever said or done is viewed differently and there is no chance that you can justify anything anymore

For PCI compliance, you could face legal liabilities by all affected parties. In the case of our PCI account -- you would be PERSONALLY responsible and action taken against you as an individual. Even if you had no idea that X Y Z had happened or would happen. However, under our realistic context, you would not sustain that tree falling

Also, just for the first action -- even with normal circumsatnces, willful misconduct or fraud are just the start of legal issus

So #3 is basically... your ability to sustain yourself against duress or other risks to you that you must do until you can no longer do so safely

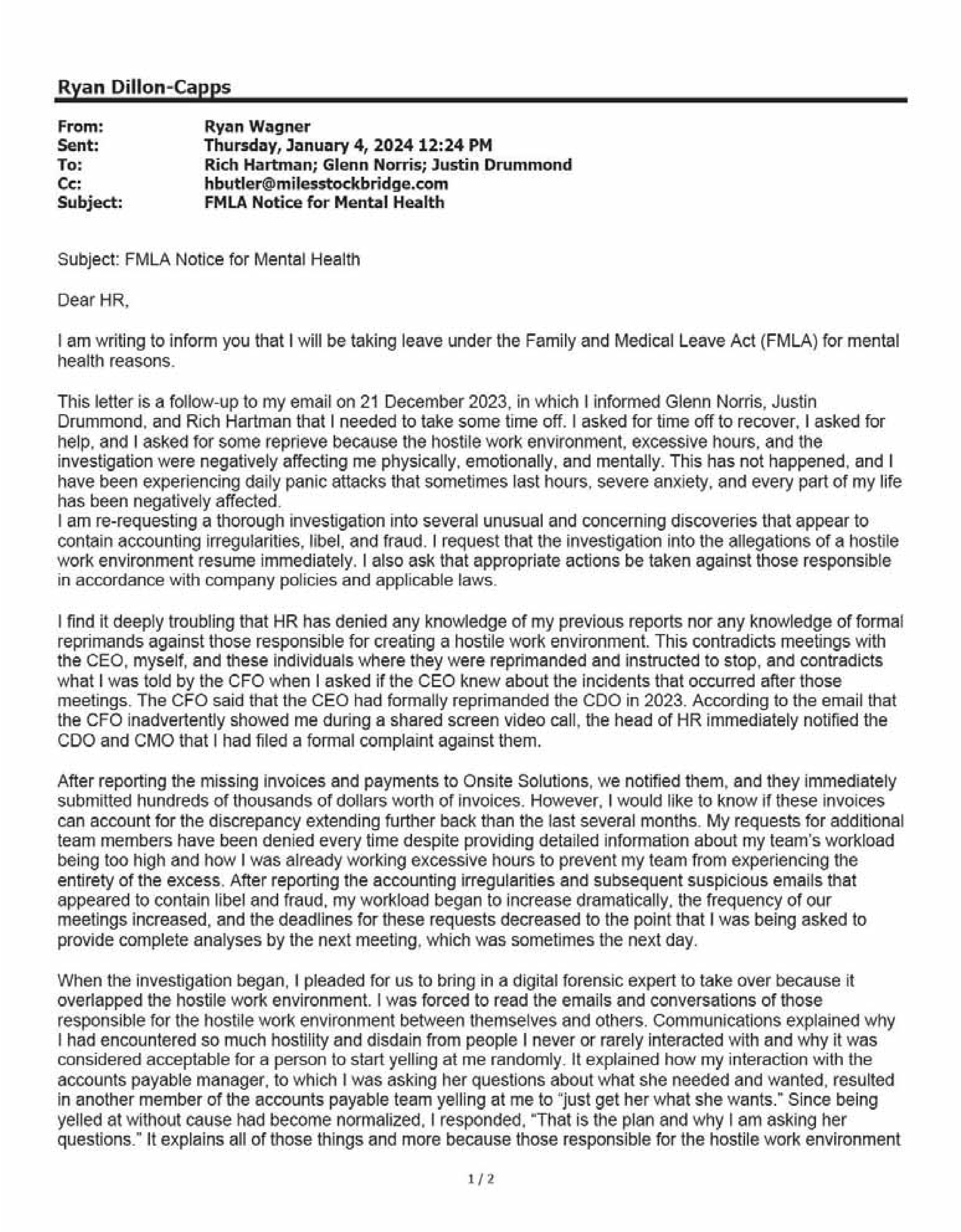
this is why I can't give it to Darren

it would be unfair to him and realistically I don't think he would be able to perform that duty while under duress

Justin Drummond Tuesday 7:46 PM

I am traveling tomorrow through the end of the week. We can work on the iPad next week

Exhibit 5C



Ryan Dillon-Capps

From:	**Ryan Wagner**
Sent:	**Thursday, January 4, 2024 12:24 PM**
To:	**Rich Hartman; Glenn Norris; Justin Drummond**
Cc:	**hbutler@milesstockbridge.com**
Subject:	**FMLA Notice for Mental Health**

Subject: FMLA Notice for Mental Health

Dear HR,

I am writing to inform you that I will be taking leave under the Family and Medical Leave Act (FMLA) for mental health reasons.

This letter is a follow-up to my email on 21 December 2023, in which I informed Glenn Norris, Justin Drummond, and Rich Hartman that I needed to take some time off. I asked for time off to recover, I asked for help, and I asked for some reprieve because the hostile work environment, excessive hours, and the investigation were negatively affecting me physically, emotionally, and mentally. This has not happened, and I have been experiencing daily panic attacks that sometimes last hours, severe anxiety, and every part of my life has been negatively affected.
I am re-requesting a thorough investigation into several unusual and concerning discoveries that appear to contain accounting irregularities, libel, and fraud. I request that the investigation into the allegations of a hostile work environment resume immediately. I also ask that appropriate actions be taken against those responsible in accordance with company policies and applicable laws.

I find it deeply troubling that HR has denied any knowledge of my previous reports nor any knowledge of formal reprimands against those responsible for creating a hostile work environment. This contradicts meetings with the CEO, myself, and these individuals where they were reprimanded and instructed to stop, and contradicts what I was told by the CFO when I asked if the CEO knew about the incidents that occurred after those meetings. The CFO said that the CEO had formally reprimanded the CDO in 2023. According to the email that the CFO inadvertently showed me during a shared screen video call, the head of HR immediately notified the CDO and CMO that I had filed a formal complaint against them.

After reporting the missing invoices and payments to Onsite Solutions, we notified them, and they immediately submitted hundreds of thousands of dollars worth of invoices. However, I would like to know if these invoices can account for the discrepancy extending further back than the last several months. My requests for additional team members have been denied every time despite providing detailed information about my team's workload being too high and how I was already working excessive hours to prevent my team from experiencing the entirety of the excess. After reporting the accounting irregularities and subsequent suspicious emails that appeared to contain libel and fraud, my workload began to increase dramatically, the frequency of our meetings increased, and the deadlines for these requests decreased to the point that I was being asked to provide complete analyses by the next meeting, which was sometimes the next day.

When the investigation began, I pleaded for us to bring in a digital forensic expert to take over because it overlapped the hostile work environment. I was forced to read the emails and conversations of those responsible for the hostile work environment between themselves and others. Communications explained why I had encountered so much hostility and disdain from people I never or rarely interacted with and why it was considered acceptable for a person to start yelling at me randomly. It explained how my interaction with the accounts payable manager, to which I was asking her questions about what she needed and wanted, resulted in another member of the accounts payable team yelling at me to "just get her what she wants." Since being yelled at without cause had become normalized, I responded, "That is the plan and why I am asking her questions." It explains all of those things and more because those responsible for the hostile work environment

Exhibit 5C

were engaging in a campaign to turn others against me and portray me as a monster who goes out of their way to make the lives of others difficult. As anyone who has spent significant time with me can tell you, this is the polar opposite of who I am.

You do not need me to be involved; I do not need to be forced to relive these events. Shannon Anderson made the complaint in August of 2021 and is available to speak to. The emails and communications provide more than enough information on everything I have already mentioned and so much more.

I appreciate your understanding and support during this time. I will contact you as soon as I have more information about my return date.

Thank you,
Ryan Wagner

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA
Growth Partners

Office 410 252 8058 x110
212 W. Padonia Rd
Timonium, MD 21093

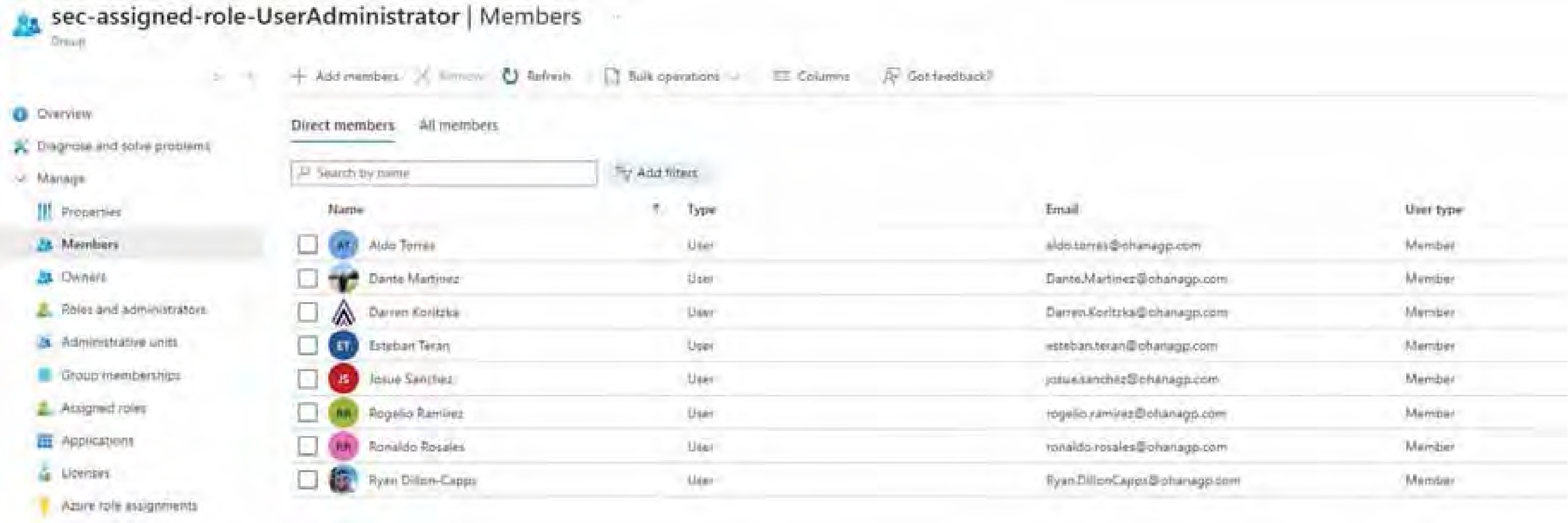
www.planetfitness.com

"Culture eats strategy for breakfast"

2 of 2

Exhibit 6

1 of 2



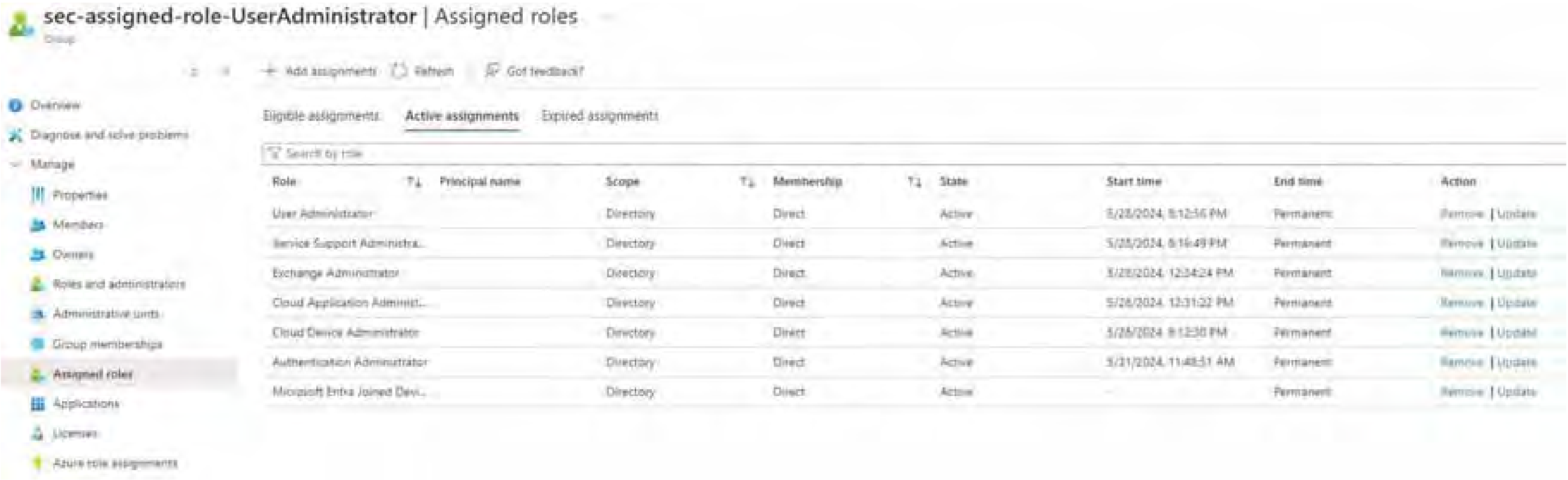
sec-assigned-role-UserAdministrator | Members

Group

	Name	Type	Email	User type
□	Aldo Torres	User	aldo.torres@ohanagp.com	Member
□	Dante Martinez	User	Dante.Martinez@ohanagp.com	Member
□	Darren Koritzka	User	Darren.Koritzka@ohanagp.com	Member
□	Esteban Teran	User	esteban.teran@ohanagp.com	Member
□	Josue Sanchez	User	josue.sanchez@ohanagp.com	Member
□	Rogelio Ramirez	User	rogelio.ramirez@ohanagp.com	Member
□	Ronaldo Rosales	User	ronaldo.rosales@ohanagp.com	Member
□	Ryan Dillon-Capps	User	Ryan.DillonCapps@ohanagp.com	Member

Exhibit 6F

2 of 2



sec-assigned-role-UserAdministrator | Assigned roles

Group

Role	Principal name	Scope	Membership	State	Start time	End time	Action
User Administrator		Directory	Direct	Active	5/28/2024, 8:12:56 PM	Permanent	Remove | Update
Service Support Administra...		Directory	Direct	Active	5/28/2024, 8:16:49 PM	Permanent	Remove | Update
Exchange Administrator		Directory	Direct	Active	5/28/2024, 12:34:24 PM	Permanent	Remove | Update
Cloud Application Administ...		Directory	Direct	Active	5/28/2024, 12:31:22 PM	Permanent	Remove | Update
Cloud Device Administrator		Directory	Direct	Active	5/28/2024, 8:12:30 PM	Permanent	Remove | Update
Authentication Administrator		Directory	Direct	Active	5/31/2024, 11:48:51 AM	Permanent	Remove | Update
Microsoft Entra Joined Devi...		Directory	Direct	Active	-	Permanent	Remove | Update

Exhibit 6G

User Administrator

PRIVILEGED

This is a privileged role. Assign the User Administrator role to users who need to do the following:

Expand table

Permission	More information
Create users	
Update most user properties for all users, including all administrators	Who can perform sensitive actions
Update sensitive properties (including user principal name) for some users	Who can perform sensitive actions
Disable or enable some users	Who can perform sensitive actions
Delete or restore some users	Who can perform sensitive actions
Create and manage user views	
Create and manage all groups	
Assign and read licenses for all users, including all administrators	
Reset passwords	Who can reset passwords
Invalidate refresh tokens	Who can reset passwords
Update (FIDO) device keys	
Update password expiration policies	
Create and manage support tickets in Azure and the Microsoft 365 admin center	
Monitor service health	

Users with this role cannot do the following:

- Cannot manage MFA.
- Cannot change the credentials or reset MFA for members and owners of a role-assignable group.
- Cannot manage shared mailboxes.

Exhibit 6G

ⓘ Important

Users with this role can change passwords for people who may have access to sensitive or private information or critical configuration inside and outside of Microsoft Entra ID. Changing the password of a user may mean the ability to assume that user's identity and permissions. For example:

- Application Registration and Enterprise Application owners, who can manage credentials of apps they own. Those apps may have privileged permissions in Microsoft Entra ID and elsewhere not granted to User Administrators. Through this path a User Administrator may be able to assume the identity of an application owner and then further assume the identity of a privileged application by updating the credentials for the application.
- Azure subscription owners, who may have access to sensitive or private information or critical configuration in Azure.
- Security Group and Microsoft 365 group owners, who can manage group membership. Those groups may grant access to sensitive or private information or critical configuration in Microsoft Entra ID and elsewhere.
- Administrators in other services outside of Microsoft Entra ID like Exchange Online, Microsoft 365 Defender portal, Microsoft Purview compliance portal, and human resources systems.
- Non-administrators like executives, legal counsel, and human resources employees who may have access to sensitive or private information.

Expand table

Actions	Description
microsoft.directory/accessReviews/definitions.applications/allProperties/allTasks	Manage access reviews of application role assignments in Microsoft Entra ID
microsoft.directory/accessReviews/definitions.directoryRoles/allProperties/read	Read all properties of access reviews for Microsoft Entra role assignments
microsoft.directory/accessReviews/definitions.entitlementManagement/allProperties/allTasks	Manage access reviews for access package assignments in entitlement management
microsoft.directory/accessReviews/definitions.groups/allProperties/update	Update all properties of access reviews for membership in Security and Microsoft 365 groups, excluding role-assignable groups.

Exhibit 6G

Actions	Description
microsoft.directory/accessReviews/definitions.groups/create	Create access reviews for membership in Security and Microsoft 365 groups.
microsoft.directory/accessReviews/definitions.groups/delete	Delete access reviews for membership in Security and Microsoft 365 groups.
microsoft.directory/accessReviews/definitions.groups/allProperties/read	Read all properties of access reviews for membership in Security and Microsoft 365 groups, including role-assignable groups.
microsoft.directory/contacts/create	Create contacts
microsoft.directory/contacts/delete	Delete contacts
microsoft.directory/contacts/basic/update	Update basic properties on contacts
microsoft.directory/deletedItems.groups/restore	Restore soft deleted groups to original state
microsoft.directory/deletedItems.users/restore	Restore soft deleted users to original state
microsoft.directory/entitlementManagement/allProperties/allTasks	Create and delete resources, and read and update all properties in Microsoft Entra entitlement management
microsoft.directory/groups/assignLicense	Assign product licenses to groups for group-based licensing
microsoft.directory/groups/create	Create Security groups and Microsoft 365 groups, excluding role-assignable groups
microsoft.directory/groups/delete	Delete Security groups and Microsoft 365 groups, excluding role-assignable groups
microsoft.directory/groups/hiddenMembers/read	Read hidden members of Security groups and Microsoft 365 groups, including role-assignable groups
microsoft.directory/groups/reprocessLicenseAssignment	Reprocess license assignments for group-based licensing
microsoft.directory/groups/restore	Restore groups from soft-deleted container
microsoft.directory/groups/basic/update	Update basic properties on Security groups and Microsoft 365 groups, excluding role-assignable groups
microsoft.directory/groups/classification/update	Update the classification property on Security groups and Microsoft 365 groups, excluding role-assignable groups

Exhibit 6G

Actions	Description
microsoft.directory/groups/dynamicMembershipRule/update	Update the dynamic membership rule on Security groups and Microsoft 365 groups, excluding role-assignable groups
microsoft.directory/groups/groupType/update	Update properties that would affect the group type of Security groups and Microsoft 365 groups, excluding role-assignable groups
microsoft.directory/groups/members/update	Update members of Security groups and Microsoft 365 groups, excluding role-assignable groups
microsoft.directory/groups/onPremWriteBack/update	Update Microsoft Entra groups to be written back to on-premises with Microsoft Entra Connect
microsoft.directory/groups/owners/update	Update owners of Security groups and Microsoft 365 groups, excluding role-assignable groups
microsoft.directory/groups/settings/update	Update settings of groups
microsoft.directory/groups/visibility/update	Update the visibility property of Security groups and Microsoft 365 groups, excluding role-assignable groups
microsoft.directory/oAuth2PermissionGrants/allProperties/allTasks	Create and delete OAuth 2.0 permission grants, and read and update all properties PRIVILEGED
microsoft.directory/policies/standard/read	Read basic properties on policies
microsoft.directory/servicePrincipals/appRoleAssignedTo/update	Update service principal role assignments
microsoft.directory/users/assignLicense	Manage user licenses
microsoft.directory/users/create	Add users PRIVILEGED
microsoft.directory/users/convertExternalToInternalMemberUser	Convert external user to internal user
microsoft.directory/users/delete	Delete users PRIVILEGED
microsoft.directory/users/disable	Disable users PRIVILEGED

Exhibit 6G

Actions	Description
microsoft.directory/users/enable	Enable users PRIVILEGED
microsoft.directory/users/inviteGuest	Invite guest users
microsoft.directory/users/invalidateAllRefreshTokens	Force sign-out by invalidating user refresh tokens PRIVILEGED
microsoft.directory/users/reprocessLicenseAssignment	Reprocess license assignments for users
microsoft.directory/users/restore	Restore deleted users
microsoft.directory/users/basic/update	Update basic properties on users
microsoft.directory/users/manager/update	Update manager for users
microsoft.directory/users/password/update	Reset passwords for all users PRIVILEGED
microsoft.directory/users/photo/update	Update photo of users
microsoft.directory/users/sponsors/update	Update sponsors of users
microsoft.directory/users/usageLocation/update	Update usage location of users
microsoft.directory/users/userPrincipalName/update	Update User Principal Name of users PRIVILEGED
microsoft.azure.serviceHealth/allEntities/allTasks	Read and configure Azure Service Health
microsoft.azure.supportTickets/allEntities/allTasks	Create and manage Azure support tickets
microsoft.office365.serviceHealth/allEntities/allTasks	Read and configure Service Health in the Microsoft 365 admin center
microsoft.office365.supportTickets/allEntities/allTasks	Create and manage Microsoft 365 service requests
microsoft.office365.webPortal/allEntities/standard/read	Read basic properties on all resources in the Microsoft 365 admin center

Virtual Visits Administrator

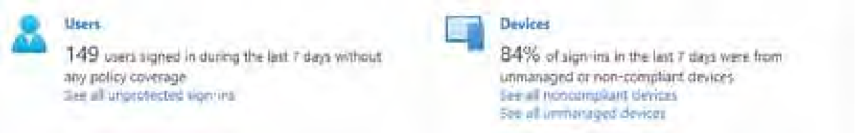
Exhibit 24C-2

From:	Ryan Wagner
Sent:	Tuesday, May 28, 2024 8:00 AM
To:	Justin Drummond; Glenn Norris
Cc:	Rich Hartman; Karen Debus; Stacey Wittelsberger (ESC); C. Victor Brick; Lynne Brick B.S.N. M.A.; Terry Woods (Planet Fitness); Earl Ihle
Subject:	Re: Full Admin Access to IT Systems to OGP President- Justin Drummond

Over the weekend, we continued working to address security issues, audit our systems, and perform tasks related to Microsoft's recommendations. This has allowed us to reduce some of the security restrictions put in place in response to the unauthorized access incident. We will continue to monitor our systems with heightened vigilance and are prepared to act quickly if additional unauthorized access is detected.

We have work remaining to do, but it would be helpful to know what Ryan Brooks was supposed to do because I have difficulty understanding the justification for his recent work.

This data is based on the last week:



Users

149 users signed in during the last 7 days without any policy coverage

See all unprotected sign-ins

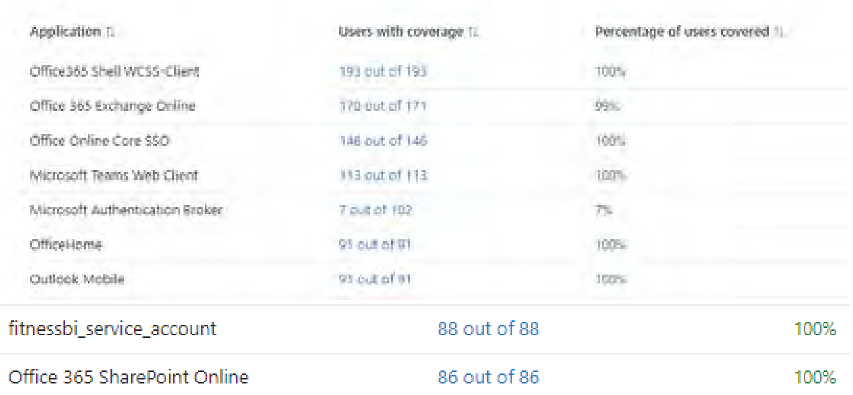
Devices

84% of sign-ins in the last 7 days were from unmanaged or non-compliant devices

See all noncompliant devices

See all unmanaged devices

This data is reflective of where we are at now.



Application ⇅	Users with coverage ⇅	Percentage of users covered ⇅
Office365 Shell WCSS-Client	193 out of 193	100%
Office 365 Exchange Online	170 out of 171	99%
Office Online Core SSO	146 out of 146	100%
Microsoft Teams Web Client	113 out of 113	100%
Microsoft Authentication Broker	7 out of 102	7%
OfficeHome	91 out of 91	100%
Outlook Mobile	91 out of 91	100%
fitnessbi_service_account	88 out of 88	100%
Office 365 SharePoint Online	86 out of 86	100%

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Sunday, May 26, 2024 8:44 PM
To: Justin Drummond <Justin.Drummond@ohanagp.com>; Glenn Norris <glenn@ohanagp.com>
Cc: Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Stacey Wittelsberger (ESC) <srector@exeterstreetcapital.com>; C. Victor Brick <Victor@ohanagp.com>; Lynne Brick B.S.N. M.A. <lynne@ohanagp.com>; Terry Woods (Planet Fitness) <Terry.Woods@ohanagp.com>; Earl Ihle <Earl.Ihle@ohanagp.com>
Subject: Re: Full Admin Access to IT Systems to OGP President- Justin Drummond

@Justin Drummond Aloha,

PCI Compliance is critical, and violations of PCI compliance will impact all of Planet Fitness. PCI DSS4 covers more than what was previously covered:

> PCI DSS requirements apply to entities with environments where account data (cardholder data and/or sensitive authentication data) is stored processed, or transmitted, and entities with environments that can impact the security of the CDE. Some PCI DSS requirements may also apply to entities with environments that do not store, process, or transmit account data – for example, entities that outsource payment operations or management of their CDE [1]. Entities that outsource their payment environments or payment operations to third parties remain responsible for ensuring that the account data is protected by the third party per applicable PCI DSS requirements.

Here is a single example for M365 and Azure

Exhibit 24C-2

M365: Intune - Manages our iPads and can impact the CDE's security.
Azure: The Kiosk platform is hosted in our Azure environment and qualifies as custom software designed for the CDE.

PCI DSS 4 mandates that access be limited to the minimum necessary for individuals to perform their job responsibilities. This principle of least privilege is why I have repeatedly requested details on the specific access needed. While Ryan Brooks is uniquely disqualified, knowing the precise requirements allows me to provide alternative solutions to ensure tasks are completed in a timely manner.

Alternatively, you can schedule a meeting with Geoff VanMastricht and me to discuss this. Geoff oversees the PCI Compliance process, and with all the information he has, he is capable of making an informed decision about whether the action you are requesting is allowed or not. Therefore, I do not foresee any issues with implementing the actions he approves.
Only Authorized Personnel can approve access, and for us, this includes Geoff and me, as we are responsible for and knowledgeable about PCI DSS 4 Compliance requirements.

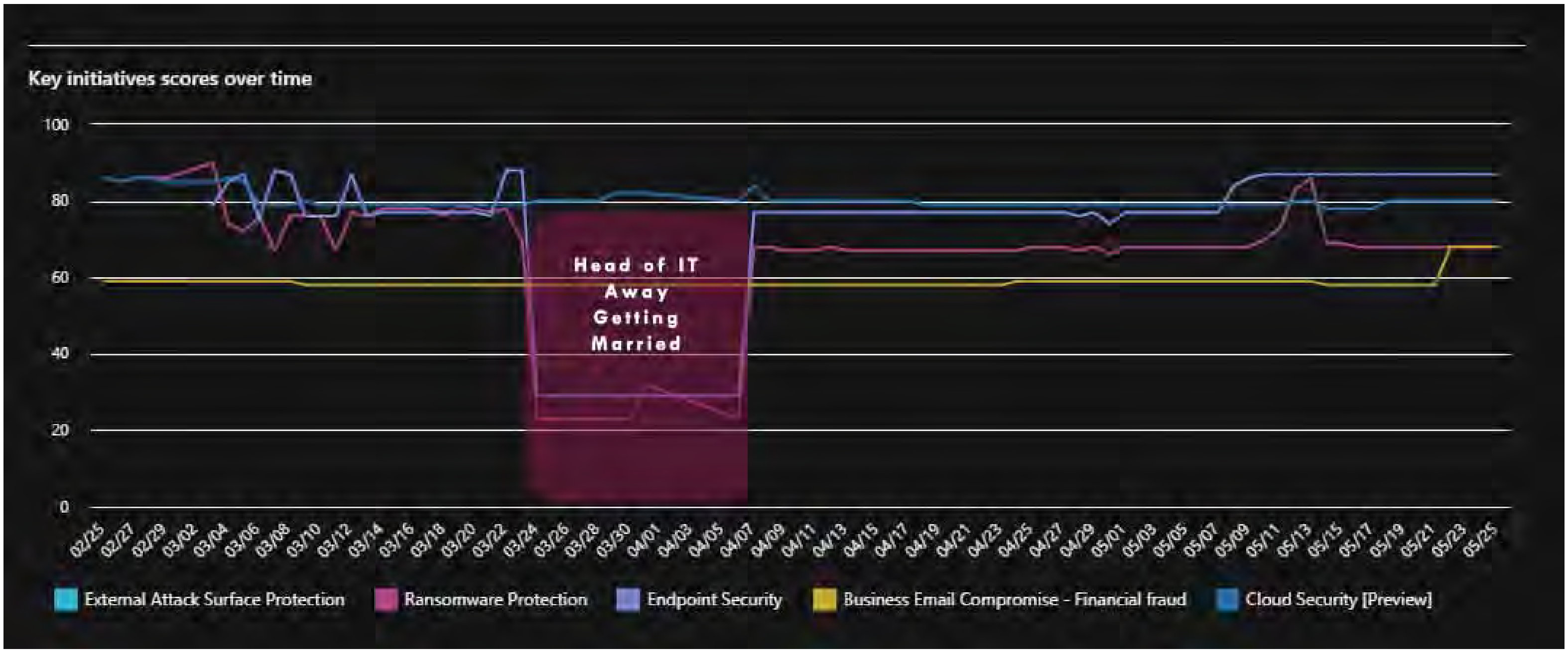
These options have been provided on multiple occasions. I cannot comply with any unlawful or unethical order.

Over the weekend and each night, I have vigilantly monitored our environment to prevent unauthorized access and continued auditing our systems. I have repaired security issues around our backups, recreated missing audits, replaced missing legal holds, and implemented further enhancements to ensure backups, logs, legal holds, and other critical items are properly protected and monitored. Fortunately, I believe our critical data remains uncompromised due to multiple layers of protection in various systems, some of which appear to have gone unnoticed.

I have made arrangements to ensure swift actions are taken to maintain or restore PCI compliance in the event that I am unavailable or unable to ensure PCI compliance is maintained.

I will not be available for discussions on Monday (a company holiday) or Tuesday as my schedule is fully booked, and I will continue to offer these options to you via email. If you inform me as to the work that Ryan Brooks urgently needs to do, then I will arrange for it to be performed. Alternatively, upon request, I will arrange a meeting with both of us to review the request together.

Additional information will be provided as soon as possible.



This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

2 of 5

Exhibit 24C-2

From: Justin Drummond <Justin.Drummond@ohanagp.com>
Sent: Friday, May 24, 2024 11:01 AM
To: Glenn Norris <glenn@ohanagp.com>; Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>
Subject: Full Admin Access to IT Systems to OGP President- Justin Drummond

Ryan,

As stated below by Glenn, the company needs to have access to our IT systems. Glenn has specifically asked you on multiple occasions to grant full admin access to all things Ohana Growth Partners related in our IT ecosystem to him and me. We do not agree with your actions as of late to block everyone but yourself from having access to our data, information, systems, etc. There should never be a single individual in any instance that has sole access for many reasons. I think you would agree to that.
It seems as though most of your concern is with Ryan Brooks and/or Glenn having access. My immediate request is that you grant me full admin access today. As President of the company, I need to be the reserve/backup for IT access and all aspects of our business.

Again, to be clear, I need to have full admin access, the exact same level as you by 5pm today. Please email me as soon as this is completed.

Thank you.

Justin Drummond
President
Ohana Growth Partners, LLC

office 410-252-8058 x214
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Friday, May 24, 2024 9:33 AM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Glenn Norris <glenn@ohanagp.com>
Subject: Response to RW's email of Unauthorized Access Incident

Ryan, since we all disagree with your actions taken to remove Ohana's & JWB Foundation's Admin rights from Ryan Brooks/Baltimore Consulting , this "trap/honeypot" email is once again an action taken by you that we disagree with and would once again demand that you cease and desist.

Our mandate from minute one when you removed Ryan Brook's Admin Rights was to make a demand to you to reverse your action and restore his admin rights. Soon thereafter, we demanded that you give full Admin rights to Justin and me- none of these demands have been implemented.

At this point, you have locked us out of the JWB Foundation admin rights- you never should have done this.

I find it interesting that you state this in your email below: "because he has been involved in our systems for so long without any supervision"- this seems to point to your dereliction of your supervisory duty.

Our stance has not changed- we want Full Admin rights restored to Ryan Brooks and add Full Admin rights to Justin and Glenn.

Your lack of communication and not following mandates from your supervisor(s) are placing you in a constant state of reprimand for insubordination.

Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Friday, May 24, 2024 8:00 AM
To: Karen Debus <karen.debus@ohanagp.com>; Justin Drummond <Justin.Drummond@ohanagp.com>; Terry Woods (Planet Fitness) <Terry.Woods@ohanagp.com>; Earl Ihle <Earl.Ihle@ohanagp.com>; C. Victor Brick <Victor@ohanagp.com>; Lynne Brick B.S.N. M.A. <lynne@ohanagp.com>; Stacey Wittelsberger (ESC) <srector@exeterstreetcapital.com>; Glenn Norris <glenn@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>

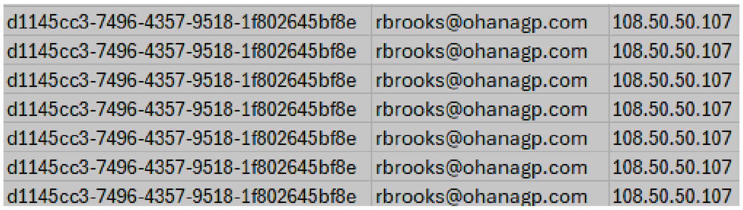
Exhibit 24C-2

Subject: Unauthorized Access Incident

I set up a trap called a honeypot for Ryan Brooks's accounts and several other areas of concern because he has been involved in our systems for so long without any supervision that I was unsure what he may have done that he could exploit. I remained on call overnight to monitor for activity. My concerns were validated on 2024, May 23, at 8:55 AM EST (12:55 UTC). when the below actions were detected:

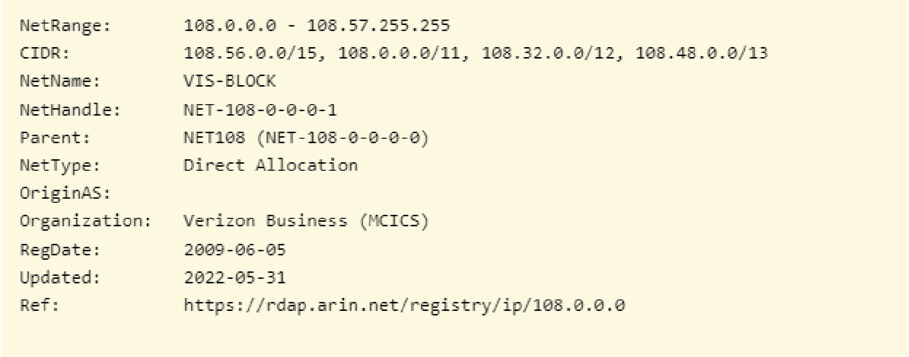
Self-service Password Management	UserManagement	Self-service password reset flow activity progress	Success	User started the mobile app code verification option
Self-service Password Management	UserManagement	Self-service password reset flow activity progress	Success	User was presented with verification options
Self-service Password Management	UserManagement	Self-service password reset flow activity progress	Success	User submitted their user ID
Self-service Password Management	UserManagement	Self-service password reset flow activity progress	Failure	User cancelled before passing the required authentication methods
Self-service Password Management	UserManagement	Self-service password reset flow activity progress	Success	User started the mobile app notification verification option
Self-service Password Management	UserManagement	Self-service password reset flow activity progress	Success	User was presented with verification options
Self-service Password Management	UserManagement	Self-service password reset flow activity progress	Success	User submitted their user ID

These actions were taken from IP Address 108.50.50.107



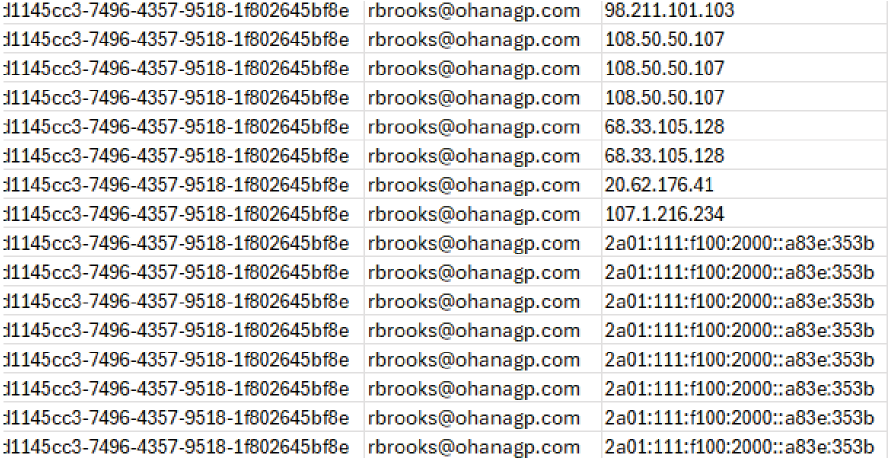
d1145cc3-7496-4357-9518-1f802645bf8e	rbrooks@ohanagp.com	108.50.50.107
d1145cc3-7496-4357-9518-1f802645bf8e	rbrooks@ohanagp.com	108.50.50.107
d1145cc3-7496-4357-9518-1f802645bf8e	rbrooks@ohanagp.com	108.50.50.107
d1145cc3-7496-4357-9518-1f802645bf8e	rbrooks@ohanagp.com	108.50.50.107
d1145cc3-7496-4357-9518-1f802645bf8e	rbrooks@ohanagp.com	108.50.50.107
d1145cc3-7496-4357-9518-1f802645bf8e	rbrooks@ohanagp.com	108.50.50.107
d1145cc3-7496-4357-9518-1f802645bf8e	rbrooks@ohanagp.com	108.50.50.107

This is a Verizon Business managed circuit.



```
NetRange:       108.0.0.0 - 108.57.255.255
CIDR:           108.56.0.0/15, 108.0.0.0/11, 108.32.0.0/12, 108.48.0.0/13
NetName:        VIS-BLOCK
NetHandle:      NET-108-0-0-0-1
Parent:         NET108 (NET-108-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Verizon Business (MCICS)
RegDate:        2009-06-05
Updated:        2022-05-31
Ref:            https://rdap.arin.net/registry/ip/108.0.0.0
```

This matches one of the IPs commonly used with the Rbrooks account.



d1145cc3-7496-4357-9518-1f802645bf8e	rbrooks@ohanagp.com	98.211.101.103
d1145cc3-7496-4357-9518-1f802645bf8e	rbrooks@ohanagp.com	108.50.50.107
d1145cc3-7496-4357-9518-1f802645bf8e	rbrooks@ohanagp.com	108.50.50.107
d1145cc3-7496-4357-9518-1f802645bf8e	rbrooks@ohanagp.com	108.50.50.107
d1145cc3-7496-4357-9518-1f802645bf8e	rbrooks@ohanagp.com	68.33.105.128
d1145cc3-7496-4357-9518-1f802645bf8e	rbrooks@ohanagp.com	68.33.105.128
d1145cc3-7496-4357-9518-1f802645bf8e	rbrooks@ohanagp.com	20.62.176.41
d1145cc3-7496-4357-9518-1f802645bf8e	rbrooks@ohanagp.com	107.1.216.234
d1145cc3-7496-4357-9518-1f802645bf8e	rbrooks@ohanagp.com	2a01:111:f100:2000::a83e:353b
d1145cc3-7496-4357-9518-1f802645bf8e	rbrooks@ohanagp.com	2a01:111:f100:2000::a83e:353b
d1145cc3-7496-4357-9518-1f802645bf8e	rbrooks@ohanagp.com	2a01:111:f100:2000::a83e:353b
d1145cc3-7496-4357-9518-1f802645bf8e	rbrooks@ohanagp.com	2a01:111:f100:2000::a83e:353b
d1145cc3-7496-4357-9518-1f802645bf8e	rbrooks@ohanagp.com	2a01:111:f100:2000::a83e:353b
d1145cc3-7496-4357-9518-1f802645bf8e	rbrooks@ohanagp.com	2a01:111:f100:2000::a83e:353b
d1145cc3-7496-4357-9518-1f802645bf8e	rbrooks@ohanagp.com	2a01:111:f100:2000::a83e:353b
d1145cc3-7496-4357-9518-1f802645bf8e	rbrooks@ohanagp.com	2a01:111:f100:2000::a83e:353b

Exhibit 24C-2

When a business experiences unauthorized access to its systems, who we report the incident to varies based on the nature and severity of the event. The good news is that once he tripped the honeypot I was able to take immediate action to prevent further actions using the methods used to gain access. In addition, the account no longer had any access or contents that it previously had, and the logs do not detect any other successful intrusion.

Based on what we know, I need to ask one uncomfortable question.

Could anyone have directed Ryan Brooks to perform these actions?

Just so you know, if someone had told him that he was authorized, anyone following up on this investigation would no longer be looking at Ryan Brooks for unauthorized access.
However, this could start a PCI compliance investigation with the named person being the focus of that investigation.

If Ryan Brooks could have mistaken something, I need to know immediately before the investigation reveals it.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

Exhibit 24K

From:	Ryan Wagner
Sent:	Tuesday, June 4, 2024 1:52 PM
To:	LeeAnn Hartman
Cc:	Dante Martinez; Rogelio Ramirez; Darren Koritzka
Subject:	Viva Goals Suite License & Dynamic License update (FYI)
Attachments:	Your Microsoft Viva Suite subscription no longer has recurring billing; Your Microsoft order on June 4, 2024; The number of licenses for your Microsoft Viva Suite subscription has changed

@LeeAnn Hartman We are slowly moving everything over to the correct MCA billing profile. Attached is us disabling the autorenewal for the incorrect account, and adding the missing licenses to the correct MCA account.

We discovered there were missing licenses while setting up dynamic licenses for leadership roles (directors, VP, C-level, president)

This should remove most situations where people would have previously needed to come to you for an additional license, as dynamic licensing will automatically remove licenses dynamically managed for inactive users and then assign them for the active ones. However, this round of improvements does not include the system automatically buying them as we did not want a mistake to result in a surge of unexpected costs.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093

www.planetfitness.com

"Culture eats strategy for breakfast"

Exhibit 12F-3

RDC-OHANA

From:	Ryan Wagner
Sent:	Wednesday, June 12, 2024 3:36 PM
To:	Glenn Norris; Rich Hartman; Justin Drummond
Cc:	Stacey Wittelsberger (ESC); C. Victor Brick; Lynne Brick B.S.N. M.A.; Terry Woods (Planet Fitness); Earl Ihle
Subject:	Re: NO SUBJECT LINE

@Glenn Norris This situation highlights why having an attorney who advises us in good faith, honestly, and transparently is crucial.

I have the right to disclose what I want, when I want, to whomever I want about my FMLA. It is not a free-for-all disclosure; knowing I am out sick or taking FMLA does not entitle anyone to access my medical records, HR information, or anything beyond what I have provided. I might choose to inform them this time, but next time I may not, and that information cannot be disclosed by someone else.

The citations provided are actual legal citations formatted correctly.

For months, you have rejected objective data and facts, stating that you disagree with me. However, you are not disagreeing with me; you are disagreeing with objective facts. These are the actual laws in violation.

Similarly, PCI compliance requires us to enforce the principle of least privilege, and PCI DSS v4 applies not only to the direct elements of the CDE but to anything that could impact its security, including infrastructure. Similar concepts have long been applied to our network segmentation. Any device connected to a PCI-compliant network must comply. If that device connects to others, the compliance requirement extends to all connected devices. By influencing the security of the iPads, the chain extends similarly under PCI DSS v4.

@Justin Drummond, Page 5 is a good starting point for understanding this concept. As you go through the document, the concepts introduced in the first few pages should be applied consistently. Another common compliance concept, though not always explicitly stated, is that when there is ambiguity, the standard to meet is higher in favor of protection. A similar principle applies in legal areas involving emergency injunctive orders by determining which side will incur more harm, with one side bearing a larger burden akin to a legal handicap. In PCI compliance, protection is prioritized, and the greater burden of proof lies with actions that might cause a violation. The likelihood of risk influences PCI decisions.

When Glenn refuses to provide any information about what Ryan Brooks is going to do, it leaves me with inadequate information to apply the principle of least privilege, resulting in an instant violation. No PCI QSA or registered assessor would side with Glenn or Ohana in this case. Even if everything else is wrong, failing to meet that requirement puts us in violation. Regulations are not about perfection but about demonstrating good faith efforts to meet these regulations. That is why we need not agree in our decisions because you will be held to your decisions, and I held to my own. As long as you can explain the logic applied and how it aligns with the intentions of PCI DSS 4 during an audit, if your decision differs from mine you should be okay.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner

Exhibit 12F-3

Vice President of IT
Ohana Growth Partners, LLC

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093

www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Wednesday, June 12, 2024 3:03 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Stacey Wittelsberger (ESC) <srector@exeterstreetcapital.com>; C. Victor Brick <Victor@ohanagp.com>; Lynne Brick B.S.N. M.A. <lynne@ohanagp.com>; Terry Woods (Planet Fitness) <Terry.Woods@ohanagp.com>; Earl Ihle <Earl.Ihle@ohanagp.com>
Subject: RE: NO SUBJECT LINE

You had already emailed them of your leave , not sure I understand?

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

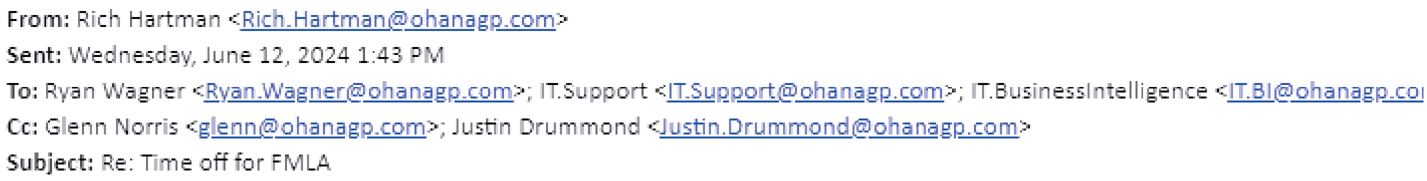
office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Wednesday, June 12, 2024 2:59 PM
To: Glenn Norris <glenn@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Stacey Wittelsberger (ESC) <srector@exeterstreetcapital.com>; C. Victor Brick <Victor@ohanagp.com>; Lynne Brick B.S.N. M.A. <lynne@ohanagp.com>; Terry Woods (Planet Fitness) <Terry.Woods@ohanagp.com>; Earl Ihle <Earl.Ihle@ohanagp.com>
Subject: Re: NO SUBJECT LINE

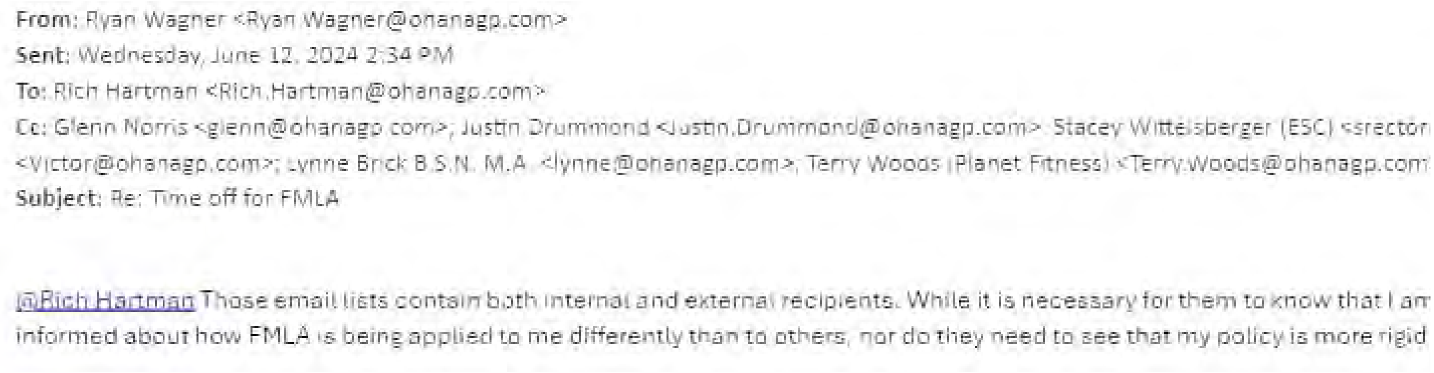
@Glenn Norris Rich sent his email to IT.Support, which contains individuals from Cielo. It is also inappropriate for internal team members to be included within IT.Support and IT.BusinessIntelligence.

Exhibit 12F-3



From: Rich Hartman <Rich.Hartman@ohanagp.com>
Sent: Wednesday, June 12, 2024 1:43 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>; IT.Support <IT.Support@ohanagp.com>; IT.BusinessIntelligence <IT.BI@ohanagp.co
Cc: Glenn Norris <glenn@ohanagp.com>; Justin Drummond <Justin.Drummond@ohanagp.com>
Subject: Re: Time off for FMLA

The email uses the mention of Rich Hartman and is addressed TO him.



From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Wednesday, June 12, 2024 2:34 PM
To: Rich Hartman <Rich.Hartman@ohanagp.com>
Cc: Glenn Norris <glenn@ohanagp.com>; Justin Drummond <Justin.Drummond@ohanagp.com>; Stacey Wittelsberger (ESC) <srector
<Victor@ohanagp.com>; Lynne Brick B.S.N. M.A. <lynne@ohanagp.com>; Terry Woods (Planet Fitness) <Terry.Woods@ohanagp.com
Subject: Re: Time off for FMLA

@Rich Hartman Those email lists contain both internal and external recipients. While it is necessary for them to know that I am
informed about how FMLA is being applied to me differently than to others, nor do they need to see that my policy is more rigid

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Wednesday, June 12, 2024 2:53 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Stacey Wittelsberger (ESC) <srector@exeterstreetcapital.com>; C. Victor Brick <Victor@ohanagp.com>; Lynne Brick B.S.N. M.A. <lynne@ohanagp.com>; Terry Woods (Planet Fitness) <Terry.Woods@ohanagp.com>; Earl Ihle <Earl.Ihle@ohanagp.com>
Subject: NO SUBJECT LINE

Ryan, I did not send the email of FMLA in the SUBJECT LINE. It was not initially sent to outsiders by me- you kept the subject line the same when responding to outsiders ?

My initial email was to you and Justin only. Asking if you would meet with Hartman Associates at 1230.

Exhibit 12F-3

Hope you are feeling better, Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Wednesday, June 12, 2024 2:34 PM
To: Rich Hartman <Rich.Hartman@ohanagp.com>
Cc: Glenn Norris <glenn@ohanagp.com>; Justin Drummond <Justin.Drummond@ohanagp.com>; Stacey Wittelsberger (ESC) <srector@exeterstreetcapital.com>; C. Victor Brick <Victor@ohanagp.com>; Lynne Brick B.S.N. M.A. <lynne@ohanagp.com>; Terry Woods (Planet Fitness) <Terry.Woods@ohanagp.com>; Earl Ihle <Earl.Ihle@ohanagp.com>
Subject: Re: Time off for FMLA

@Rich Hartman Those email lists contain both internal and external recipients. While it is necessary for them to know that I am taking FMLA leave, they do not need to be informed about how FMLA is being applied to me differently than to others, nor do they need to see that my policy is more rigid compared to policies for other types of leave.

Additionally, I provided notification the exact minute I became aware that I needed to take leave. This makes any accusation of untimely notification baseless.

Legal Citations:
Federal Law:

1. **Family and Medical Leave Act (FMLA), 29 U.S.C. § 2615(a)**
    - This section prohibits employers from interfering with, restraining, or denying the exercise of or the attempt to exercise any right provided under the FMLA.

1. **Family and Medical Leave Act (FMLA) Regulations, 29 C.F.R. § 825.500(g)**
    - This regulation requires that employers maintain the confidentiality of FMLA records and treat them as medical records, which should be maintained separately from regular personnel files and disclosed only on a need-to-know basis.

3. **Family and Medical Leave Act (FMLA) Regulations, 29 C.F.R. § 825.220(c)**
    - This regulation prohibits employers from discriminating against employees for taking FMLA leave and ensures that the terms and conditions of FMLA leave are not more stringent than those for other types of leave.

4. **Family and Medical Leave Act (FMLA) Regulations, 29 C.F.R. § 825.302(d)**
    - This regulation specifies that employees must provide notice of the need for FMLA leave as soon as practicable, typically within the same or next business day of learning of the need for leave.

Exhibit 12F-3

Maryland Law:

1. **Maryland Healthy Working Families Act, Md. Code, Labor and Employment § 3-1305**

   o This state law requires that employers keep health information related to employee leave confidential and prohibits the dissemination of such information except under specific circumstances.

1. **Maryland Healthy Working Families Act, Md. Code, Labor and Employment § 3-1306**

   o This law stipulates that employers cannot implement policies that are more restrictive for sick and safe leave than for other types of leave, ensuring equal treatment.

3. **Maryland Fair Employment Practices Act, Md. Code, State Government § 20-606**

   o This act prohibits discrimination in employment on the basis of an individual's use of leave, ensuring that leave policies are applied uniformly without bias.

By failing to maintain the confidentiality of my FMLA leave details, revealing differential treatment in the application of FMLA policies, and making my FMLA policy more rigid than those for other types of leave, these actions may constitute violations of both federal and state laws regarding the confidentiality, non-discriminatory application of leave policies, and equal treatment of leave policies.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Rich Hartman <Rich.Hartman@ohanagp.com>
Sent: Wednesday, June 12, 2024 1:43 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>; IT.Support <IT.Support@ohanagp.com>; IT.BusinessIntelligence <IT.BI@ohanagp.com>
Cc: Glenn Norris <glenn@ohanagp.com>; Justin Drummond <Justin.Drummond@ohanagp.com>
Subject: Re: Time off for FMLA

As mentioned in my email to you on January 25, 2024,

"I want to reiterate the requirement that you provide advanced notice to Glenn and to me as soon as you become aware of the need to take leave. Our regular working hours are normally an 8 hour window between 7 am and 6 pm. If at any point during those regular working hours you realize that you are in need of leave, you can send an email, copying me and Glenn, simply stating that you are going to be taking FMLA beginning at a particular day/time and that you anticipate returning to work at a particular day/time."

FMLA hours are tracked by HR. Email Glenn and me the date and number of hours. Thank you

Exhibit 12F-3

Rich Hartman
VP of People and Culture
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x114
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Wednesday, June 12, 2024 7:00 AM
To: IT.Support <IT.Support@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; IT.BusinessIntelligence <IT.BI@ohanagp.com>
Cc: Glenn Norris <glenn@ohanagp.com>; Justin Drummond <Justin.Drummond@ohanagp.com>
Subject: Time off for FMLA

@IT.Support @IT.BI Just so you know, I am taking FMLA time for leave. Please allow for extra time if you need anything from me. If there is a critical issue involving security or other imminent risk. Contact Darren. Darren will have additional instructions that will apply if necessary.

@Rich Hartman Please let me know how you want the time tracked. I assume the hours already worked will apply directly to this week? pay period? Please provide me with the written policy explaining how it is used against existing hours.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

Exhibit 19A

From:	**Ryan Wagner**
Sent:	**Tuesday, May 21, 2024 1:16 PM**
To:	**Glenn Norris**
Cc:	**Justin Drummond**
Subject:	**Ryan Brooks - More Info Needed**

@Glenn Norris, I hope you're doing well. I am seeking clarification regarding your directive to retain Ryan Brooks in the IT Department. When we talked today, you expressed a specific need for his services, despite my concerns about his performance and our compliance requirements.

In addition, As part of our compliance with PCI DSS 4 standards, which I recently certified after significant efforts, every team member must meet the requirements. Ryan Brooks' refusal to follow proper procedures and complete the required upskill training posed a substantial obstacle to maintaining PCI DSS 4 unless he is able to do the things that I have required of him.

To clarify:

1. **Security Training**: Ryan has not completed the mandatory security training, which disqualifies him from being employed as a software engineer under PCI DSS 4 standards.

2. **Code Review Process**: He has been unable to participate in the code review process, making him unsuitable for automation or SQL work.

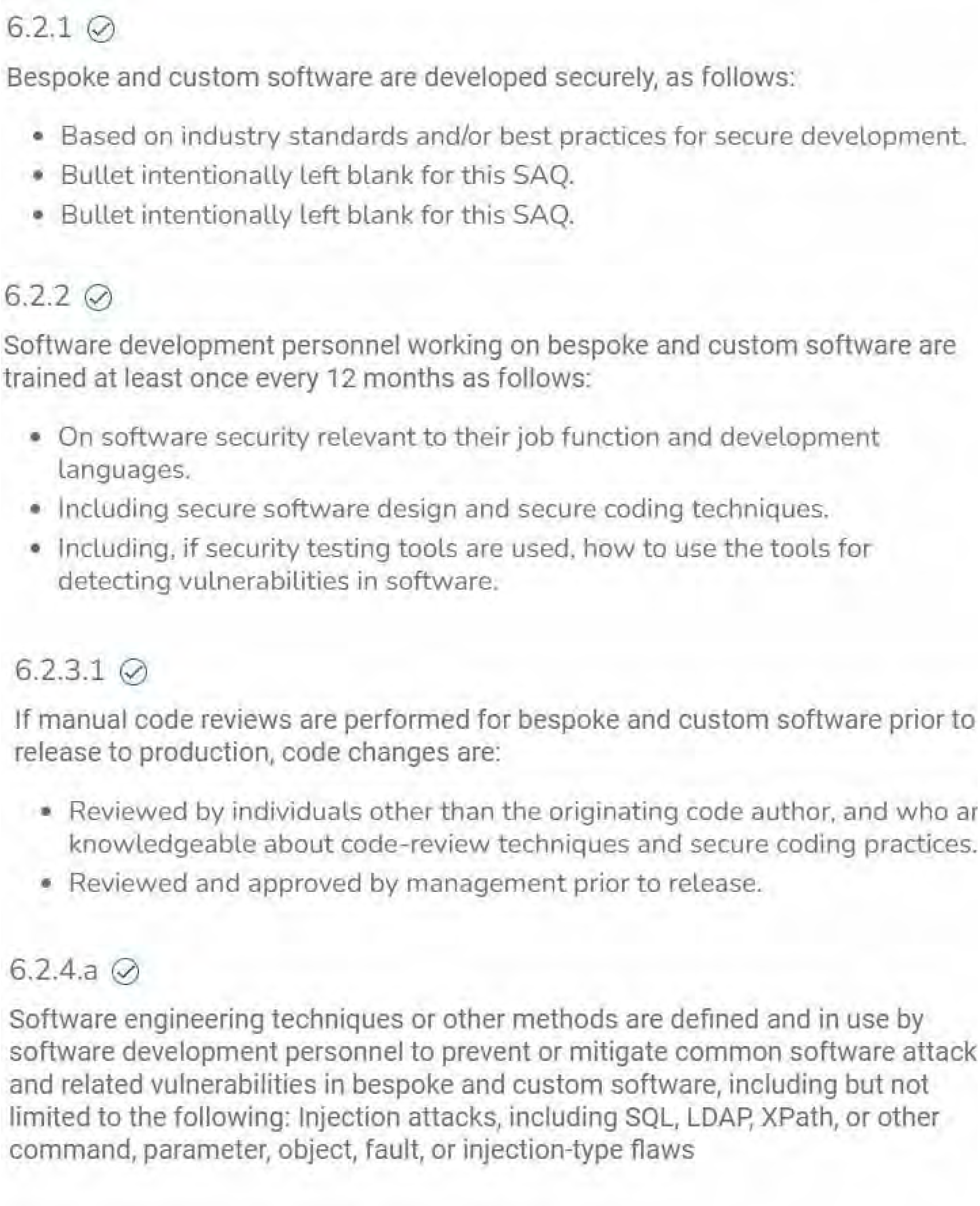
3. **Change Control Review Board**: Ryan's lack of participation in the change control review board precludes him from performing any sysadmin tasks or handling M365 or Azure responsibilities.

Given these compliance issues, retaining Ryan to work in these areas conflicts with the PCI DSS 4 standards. His non-compliance and refusal to adhere to required protocols undermine our efforts to maintain these critical standards.

Please provide specific details regarding the necessity of retaining Ryan's services and ensure that it does not conflict with our PCI DSS 4 compliance requirements. I would like you to know that understanding your rationale and how it aligns with these standards is essential for moving forward.

Thank you for your attention to this matter. I look forward to your response to resolve this issue in compliance with our obligations.

Exhibit 19A



6.2.1 ✓

Bespoke and custom software are developed securely, as follows:

- Based on industry standards and/or best practices for secure development.
- Bullet intentionally left blank for this SAQ.
- Bullet intentionally left blank for this SAQ.

6.2.2 ✓

Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows:

- On software security relevant to their job function and development languages.
- Including secure software design and secure coding techniques.
- Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.

6.2.3.1 ✓

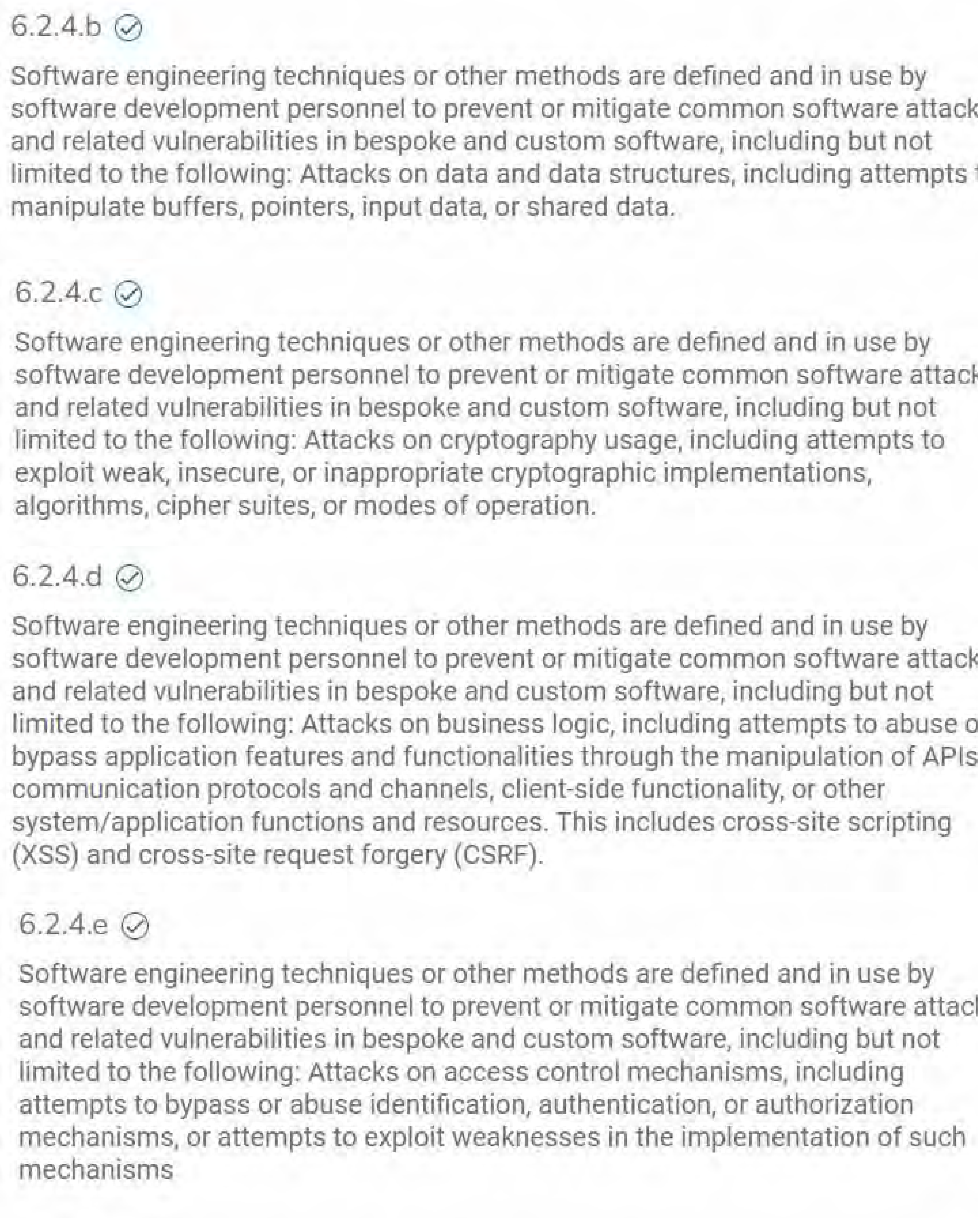
If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are:

- Reviewed by individuals other than the originating code author, and who ar knowledgeable about code-review techniques and secure coding practices.
- Reviewed and approved by management prior to release.

6.2.4.a ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws

Exhibit 19A



6.2.4.b ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on data and data structures, including attempts t manipulate buffers, pointers, input data, or shared data.

6.2.4.c ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation.

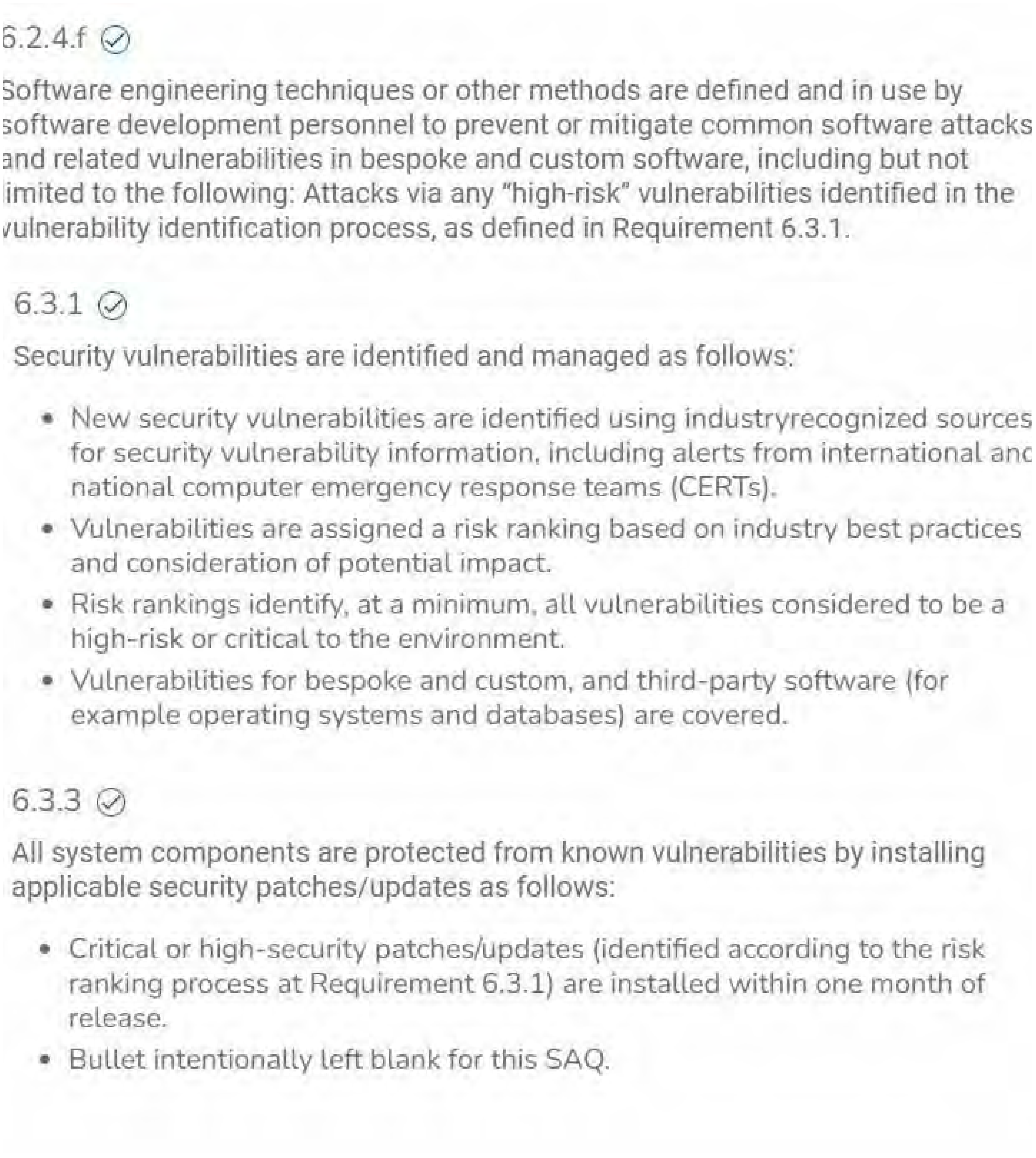
6.2.4.d ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on business logic, including attempts to abuse o bypass application features and functionalities through the manipulation of APIs communication protocols and channels, client-side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF).

6.2.4.e ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attac and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms

Exhibit 19A



6.2.4.f ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks via any "high-risk" vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1.

6.3.1 ✓

Security vulnerabilities are identified and managed as follows:

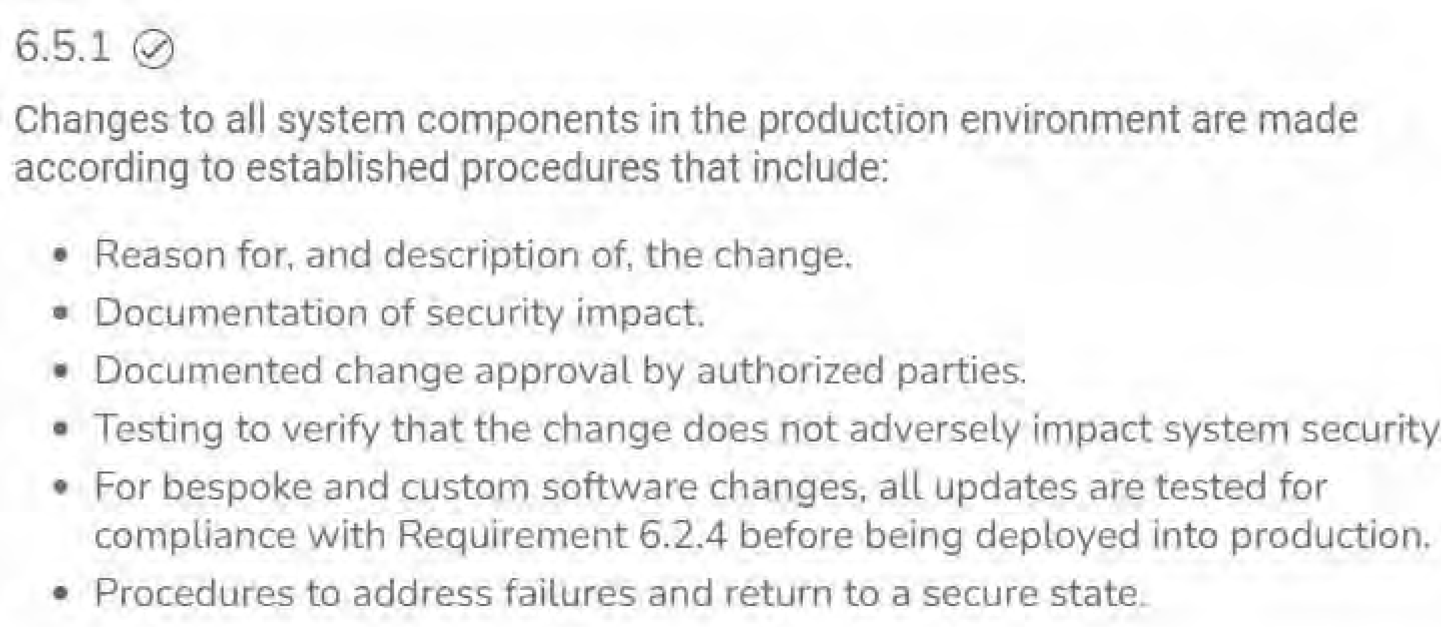
- New security vulnerabilities are identified using industryrecognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).
- Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.
- Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.
- Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.

6.3.3 ✓

All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows:

- Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release.
- Bullet intentionally left blank for this SAQ.

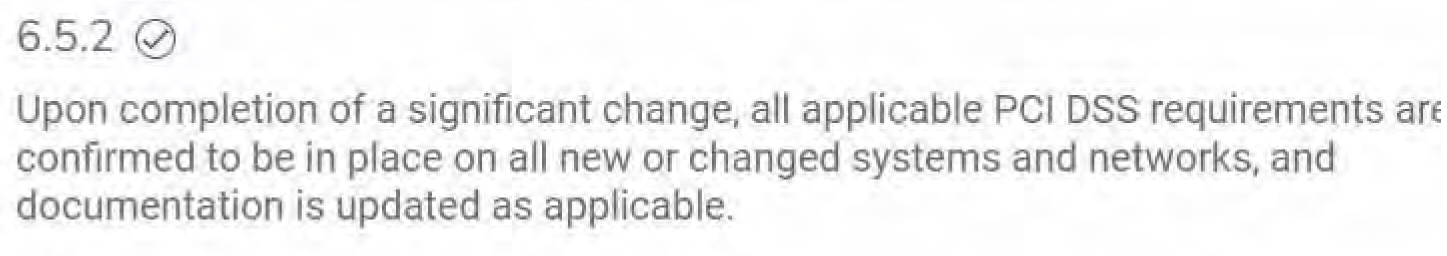
Exhibit 19A



6.5.1 ✓

Changes to all system components in the production environment are made according to established procedures that include:

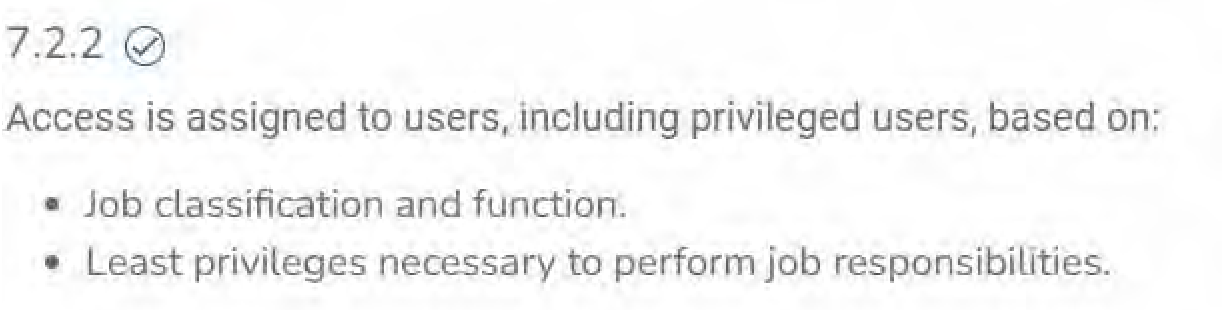
- Reason for, and description of, the change.
- Documentation of security impact.
- Documented change approval by authorized parties.
- Testing to verify that the change does not adversely impact system security
- For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production.
- Procedures to address failures and return to a secure state.



6.5.2 ✓

Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.

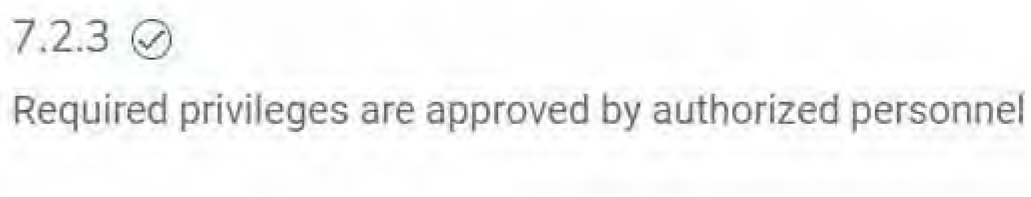
Please provide specific details regarding the necessity of retaining Ryan's services which does not conflict with our PCI DSS 4 compliance requirements. I would like you to know that understanding your rationale and how it aligns with these standards is essential for moving forward by assigning him permissions that will give him the least privileges necessary while not performing tasks listed above or otherwise in the PCI DSS 4.



7.2.2 ✓

Access is assigned to users, including privileged users, based on:

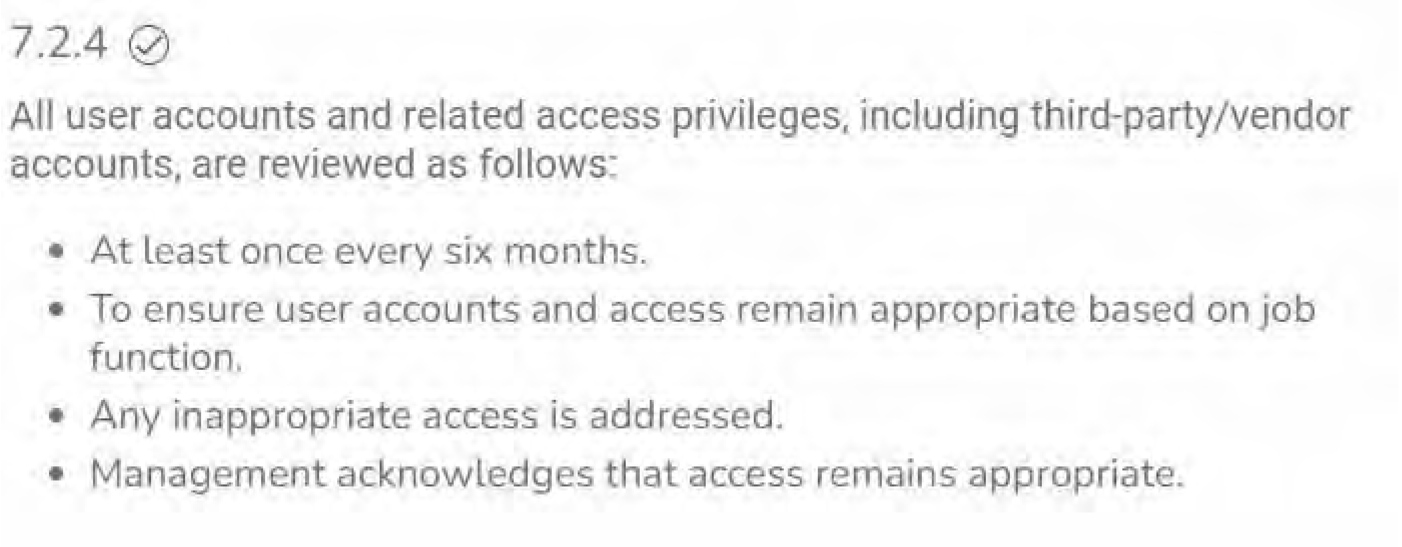
- Job classification and function.
- Least privileges necessary to perform job responsibilities.



7.2.3 ✓

Required privileges are approved by authorized personnel

Exhibit 19A



7.2.4 ✓

All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows:

- At least once every six months.
- To ensure user accounts and access remain appropriate based on job function.
- Any inappropriate access is addressed.
- Management acknowledges that access remains appropriate.

Thank you for your attention to this matter. I look forward to your response and to resolving this issue in accordance with our obligations.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093

www.planetfitness.com

“Culture eats strategy for breakfast”

Exhibit 19B

From: **Ryan Wagner**
Sent: **Tuesday, May 21, 2024 2:08 PM**
To: **Glenn Norris**
Cc: **Justin Drummond; Rich Hartman; Karen Debus; Matt Norris**
Subject: **Re: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS**

@Glenn Norris I hope this message finds you well. I appreciate your prompt response regarding Ryan Brooks' compliance and performance. I would like to address the points you raised to ensure clarity and alignment with our compliance requirements and performance expectations.

Compliance Allegations:
Regarding the compliance allegations, it is crucial to clarify that all team members, including vendors, must complete the required PCI DSS compliance training. This is a non-negotiable requirement to maintain our certification and ensure our systems' security and integrity. If Ryan was previously informed that he did not need to complete this training, that was incorrect, and I appreciate his willingness to rectify this.

Compliance Training Requirement:
Ryan must complete the PCI DSS compliance training before he can resume any work, as our attestation has already been filed.
Additional Compliance Requirements:

Beyond the training, Ryan's access has been restricted due to his lack of participation in several PCI DSS-required processes. These include:

Participation in daily standup meetings
Involvement in the change control review board
Engagement in the pipeline for code publishing
Adherence to other necessary procedures
Ryan has previously refused to engage in these processes, which are critical for maintaining our compliance. Additionally, the partial work he has completed has not met PCI DSS compliance standards, and I have had to redo this work to align with our requirements.

Access and Admin Rights:
Regarding your directive to restore Ryan's admin rights immediately, I must emphasize that any such action must comply with our PCI DSS 4 standards. Until Ryan completes the required compliance steps and demonstrates his understanding of PCI DSS requirements, he will not be able to make changes to any system as an administrator. This includes both his software engineer responsibilities and sufficient training for administration.

Next Steps:

Ryan must complete the PCI DSS compliance training immediately.
Ryan must participate in all PCI DSS required processes, including daily standups, change control review boards, and code publishing pipelines.
After Ryan completes the training and engages in these processes, we need detailed information on the specific tasks you want him to perform. This will allow us to assign him the least privileged access necessary to maintain PCI compliance.

Exhibit 19B

If you feel it would be helpful, I am open to arranging a meeting with the corporate head of security to weigh in on these items and provide additional perspective on maintaining our compliance and security standards.

Thank you for your understanding and cooperation in ensuring we maintain our compliance and security standards. I look forward to resolving this matter collaboratively.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093

www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 1:48 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>; Glenn Norris <glenn@ohanagp.com>
Subject: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

Ryan, I do not agree with your performance and compliance allegations of Ryan Brooks. I asked him if he was required by you to complete the compliance PCI tests and he was adamant that you stated months ago that he did not need to complete this. He is willing to do it. This is straight from Ryan Brooks.

Regarding his performance, we need to have a conversation on your expectations and role for BC/RB. In my opinion, he has been and still is a valued vendor for our IT needs .

Please ask Justin, Rich, Matt or Karen(and others) how they do or do not value his contribution to our IT needs.

As I stated in our call earlier today, I want his admin rights restored today. There was no discussion with me about this action – I do not approve.

SEE COMMENTS IN RED BELOW

Thank you, Glenn

Exhibit 19B

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 1:16 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>
Subject: Ryan Brooks - More Info Needed

@Glenn Norris, I hope you're doing well. I am seeking clarification regarding your directive to retain Ryan Brooks in the IT Department. When we talked today, you expressed a specific need for his services, despite my concerns about his performance and our compliance requirements.

In addition, As part of our compliance with PCI DSS 4 standards, which I recently certified after significant efforts, every team member must meet the requirements. Ryan Brooks' refusal to follow proper procedures and complete the required upskill training posed a substantial obstacle to maintaining PCI DSS 4 unless he is able to do the things that I have required of him.

To clarify:

1. Security Training: Ryan has not completed the mandatory security training, which disqualifies him from being employed as a software engineer under PCI DSS 4 standards. HE WILL DO THIS IF IT IS REQUIRED.

2. Code Review Process: He has been unable to participate in the code review process, making him unsuitable for automation or SQL work. WHAT IS THE REQUIRED TIME INVESTMENT HERE?

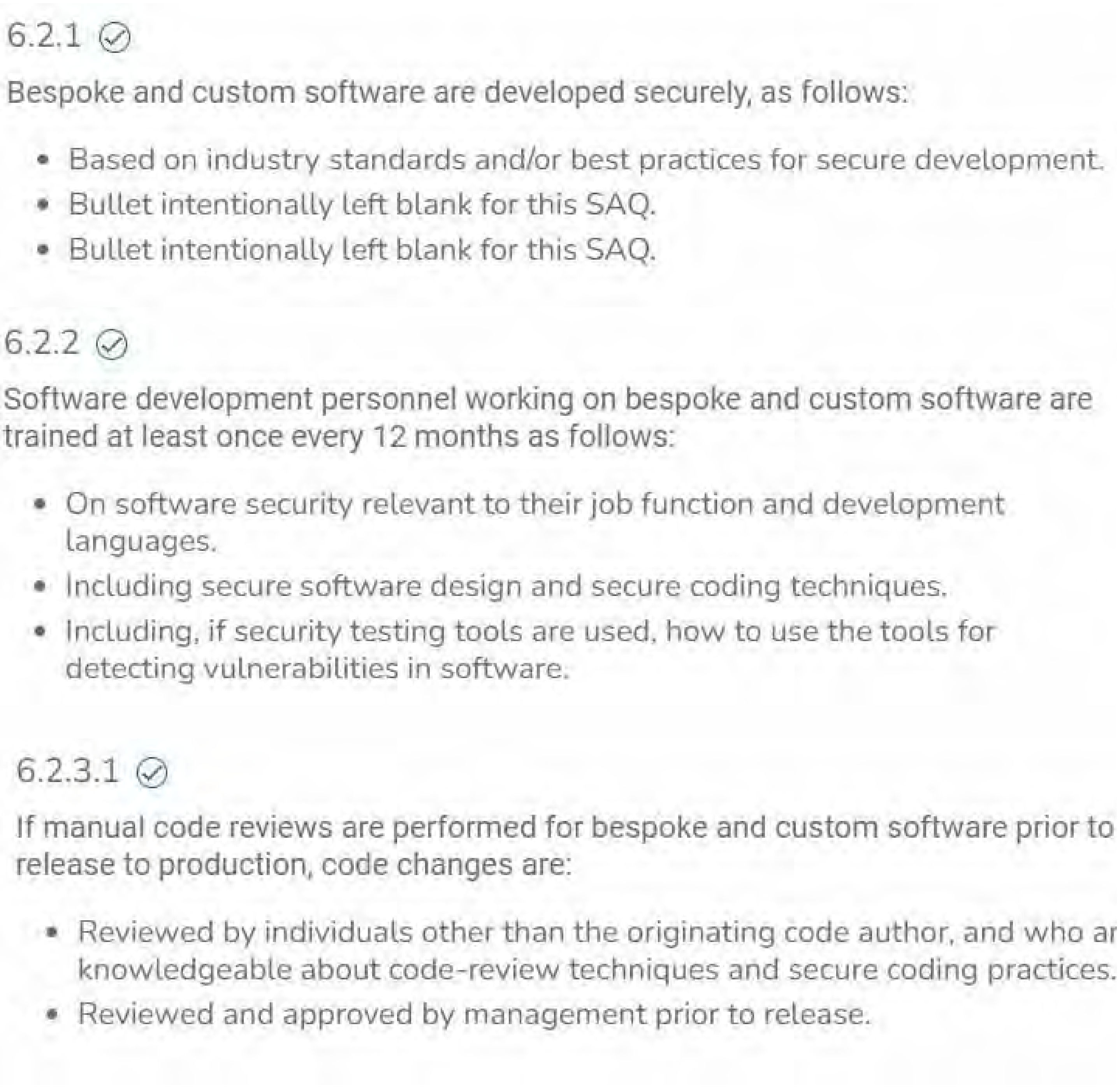
3. Change Control Review Board: Ryan's lack of participation in the change control review board precludes him from performing any sysadmin tasks or handling M365 or Azure responsibilities. HE HAS BEEN ON EVERY TUESDAY 230 CALL AND YOU GHOSTED THAT CALL ON 5-7-24 AND HE WAS IN ATTENDANCE. HE WILL NOT BE ON TODAY'S CALL SINCE YOU INADVERTANTLY FIRED HIM YESTERDAY.

Given these compliance issues, retaining Ryan to work in these areas conflicts with the PCI DSS 4 standards. His non-compliance and refusal to adhere to required protocols undermine our efforts to maintain these critical standards.

Please provide specific details regarding the necessity of retaining Ryan's services and ensure that it does not conflict with our PCI DSS 4 compliance requirements. I would like you to know that understanding your rationale and how it aligns with these standards is essential for moving forward.

Exhibit 19B

Thank you for your attention to this matter. I look forward to your response to resolve this issue in compliance with our obligations.



6.2.1 ✓

Bespoke and custom software are developed securely, as follows:

- Based on industry standards and/or best practices for secure development.
- Bullet intentionally left blank for this SAQ.
- Bullet intentionally left blank for this SAQ.

6.2.2 ✓

Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows:

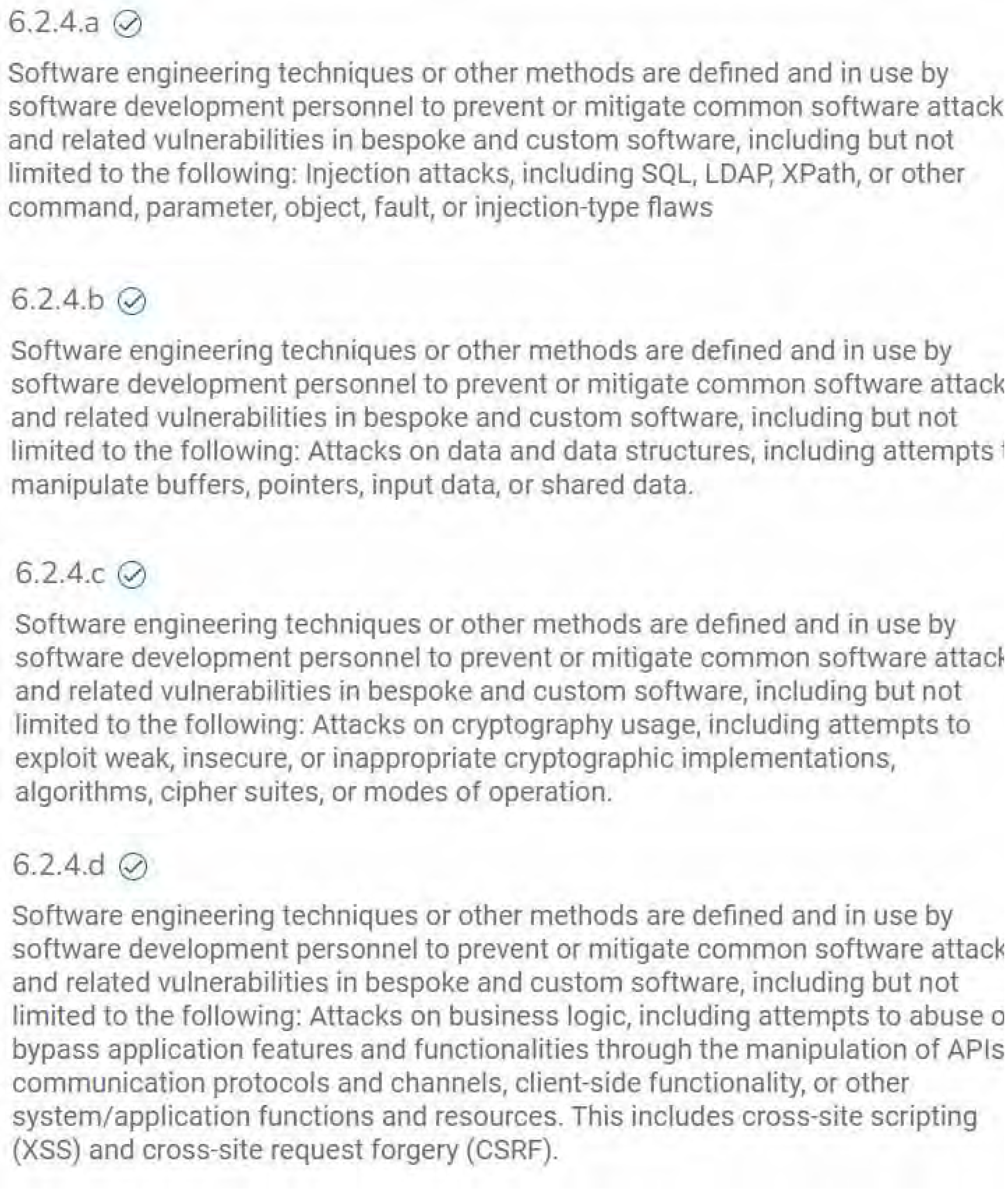
- On software security relevant to their job function and development languages.
- Including secure software design and secure coding techniques.
- Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.

6.2.3.1 ✓

If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are:

- Reviewed by individuals other than the originating code author, and who ar knowledgeable about code-review techniques and secure coding practices.
- Reviewed and approved by management prior to release.

Exhibit 19B



6.2.4.a ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws

6.2.4.b ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on data and data structures, including attempts t manipulate buffers, pointers, input data, or shared data.

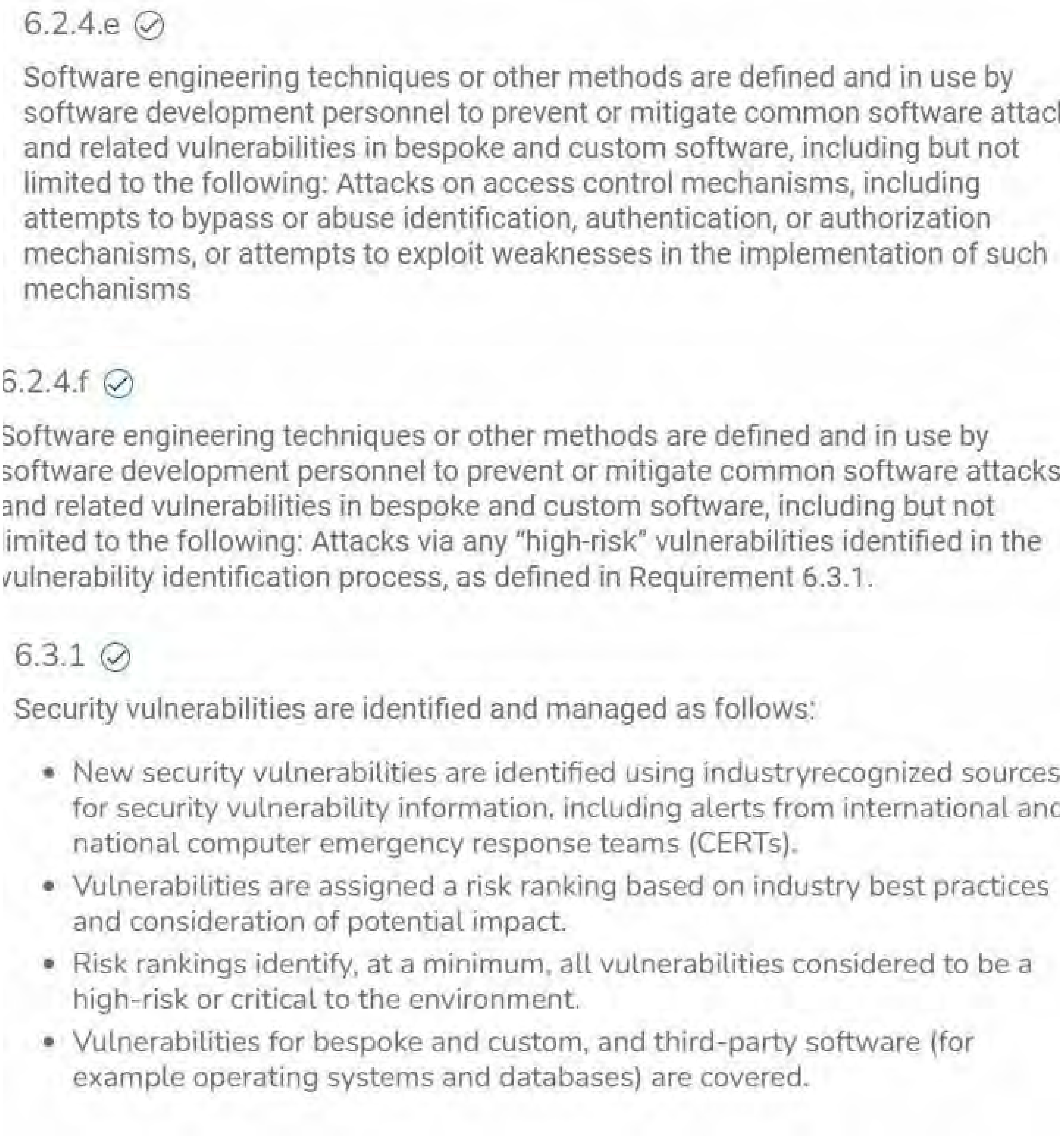
6.2.4.c ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation.

6.2.4.d ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on business logic, including attempts to abuse o bypass application features and functionalities through the manipulation of APIs communication protocols and channels, client-side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF).

Exhibit 19B



6.2.4.e ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacl and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms

6.2.4.f ✓

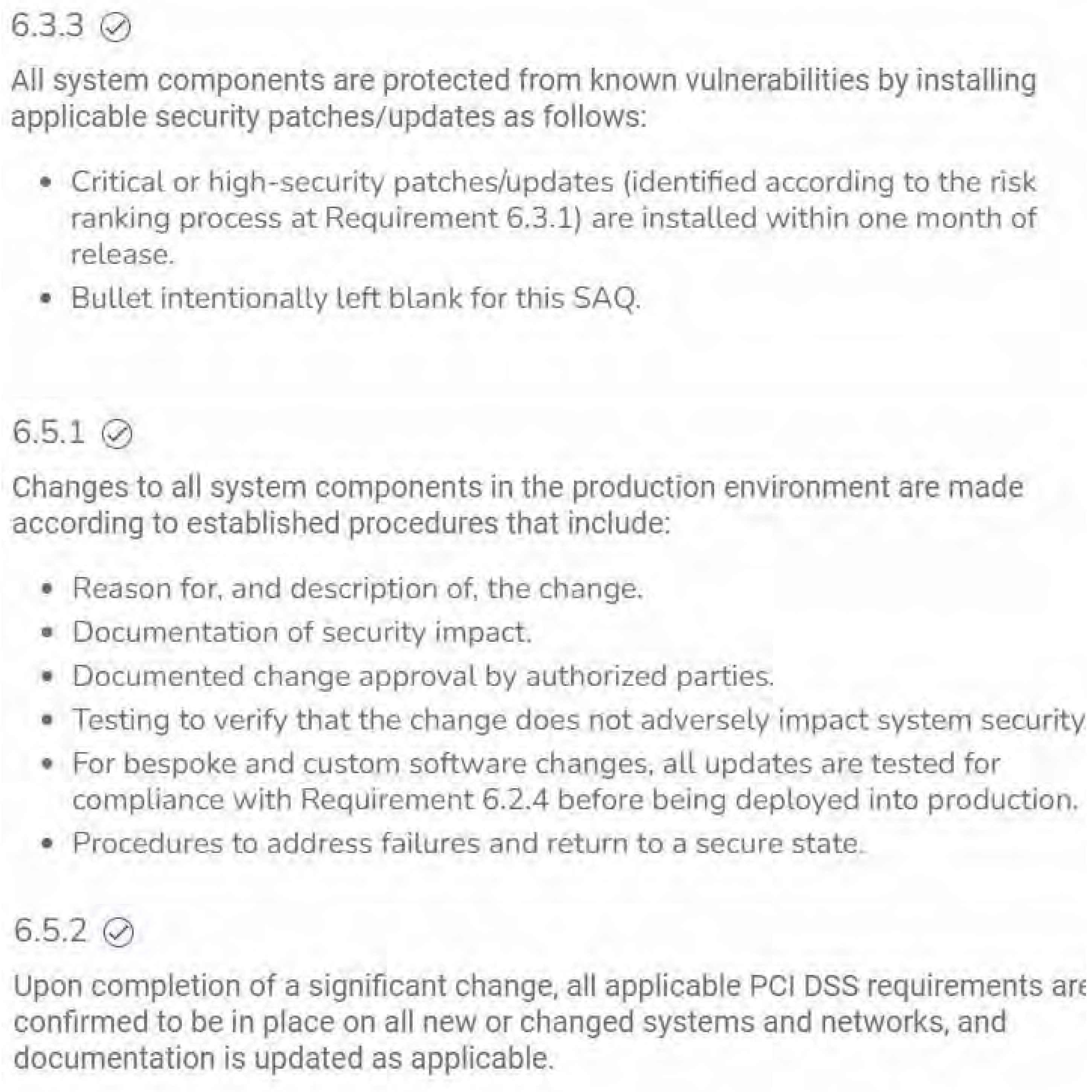
Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks via any "high-risk" vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1.

6.3.1 ✓

Security vulnerabilities are identified and managed as follows:

- New security vulnerabilities are identified using industryrecognized sources for security vulnerability information, including alerts from international anc national computer emergency response teams (CERTs).
- Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.
- Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.
- Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.

Exhibit 19B



6.3.3 ✓

All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows:

- Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release.
- Bullet intentionally left blank for this SAQ.

6.5.1 ✓

Changes to all system components in the production environment are made according to established procedures that include:

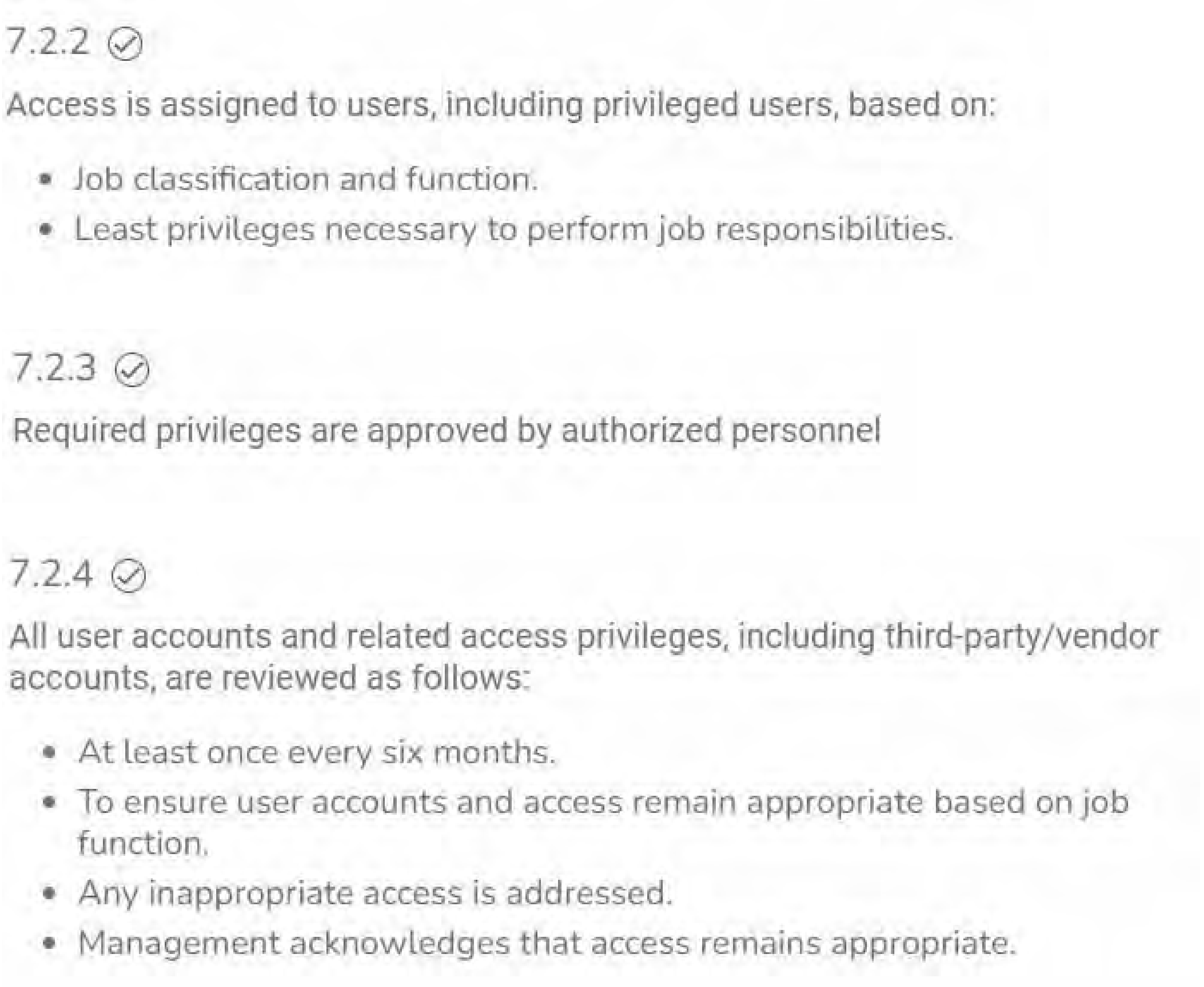
- Reason for, and description of, the change.
- Documentation of security impact.
- Documented change approval by authorized parties.
- Testing to verify that the change does not adversely impact system security
- For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production.
- Procedures to address failures and return to a secure state.

6.5.2 ✓

Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.

Please provide specific details regarding the necessity of retaining Ryan's services which does not conflict with our PCI DSS 4 compliance requirements. I would like you to know that understanding your rationale and how it aligns with these standards is essential for moving forward by assigning him permissions that will give him the least privileges necessary while not performing tasks listed above or otherwise in the PCI DSS 4.

Exhibit 19B



7.2.2 ✓

Access is assigned to users, including privileged users, based on:

- Job classification and function.
- Least privileges necessary to perform job responsibilities.

7.2.3 ✓

Required privileges are approved by authorized personnel

7.2.4 ✓

All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows:

- At least once every six months.
- To ensure user accounts and access remain appropriate based on job function.
- Any inappropriate access is addressed.
- Management acknowledges that access remains appropriate.

Thank you for your attention to this matter. I look forward to your response and to resolving this issue in accordance with our obligations.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

Exhibit 19B

OHANA
Growth Partners

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

“Culture eats strategy for breakfast”

Exhibit 19C

From:	**Ryan Wagner**
Sent:	**Tuesday, May 21, 2024 2:26 PM**
To:	**Glenn Norris**
Cc:	**Rich Hartman; Karen Debus; Justin Drummond**
Subject:	**Re: Advocating to Work - Evidence**

@Glenn Norris Thank you for your response to my earlier emails. I need to address some discrepancies and seek further clarification to ensure a clear and accurate understanding of the situation. This email is being sent because you expressed disagreement with how I have been advocating for my ability to do my job. My intent is to correct any misunderstanding and provide a comprehensive overview.

Reduction of Hours and Role:
You mentioned reducing my hours to 8 per day for my health and well-being and removing some of my responsibilities. However, these changes were implemented after I initiated FMLA on January 4th. I have no records of any communications indicating these changes before my FMLA request. In fact, I worked 48 hours straight before taking time off at the end of December, which then led to my FMLA notice being sent to HR.

Expense Reports:
I am unclear on how the timely submission of expense reports is related to my FMLA situation. Could you please provide more context regarding this point?

Upgrade of Darren’s Position:
You mentioned upgrading Darren's position. Darren is currently employed, and it has been over five months since I went on FMLA. During this period, you have been managing the department as I have been prevented from fulfilling my role. Essentially, all core functions of my job as Head of IT have been removed.

To move forward constructively, it is crucial to address the following points:

Clear documentation and communication about the changes made to my role and responsibilities.
Clarification on the relevance of the expense report submission in this context.
A comprehensive understanding of Darren's upgraded role and how it impacts the IT department's functioning.
Additionally, I have noticed a temporary restoration of some functions of my role. This seems to be an attempt to shift the perception of inefficiency from your leadership to me and isolate me from communicating with other leadership and department heads. It is important that we address these issues transparently to prevent any misunderstandings among the team.

I am committed to resolving these issues and ensuring that we maintain a collaborative work environment. I am available to discuss these matters further and work towards a resolution that upholds our compliance and operational standards.

Thank you for your attention to these matters.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner

Exhibit 19C

Vice President of IT
Ohana Growth Partners, LLC

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093

www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 2:00 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Justin Drummond <Justin.Drummond@ohanagp.com>; Glenn Norris <glenn@ohanagp.com>
Subject: FW: Advocating to Work - Evidence

Ryan, I am trying to answer your emails in a follow up of your phone call with me this morning. I cannot continue today and will not reply to any more emails today regarding your questions.

Please include Justin, Rich and Karen on any type of questions you have about FMLA. These actions below were done without FMLA being a known course of action.

Here is what I know I did prior to you requesting going on FMLA.

1. Reduce your hours to 8 hours per day- request for your health and well being.
2. Reduce the full role you once had- remove from invoices being approved and paid/ give up any type of project work.
3. Submit expense reports timely -each month.
4. Upgrade the Darren position- Darren is not working out.

I hope this clarifies your questions.

Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 12:08 PM

Exhibit 19C

To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>
Subject: Advocating to Work - Evidence

@Glenn Norris I hope this message finds you well. I am writing to clarify and provide further evidence regarding our discussion today, particularly concerning my advocacy for my ability to work.

During our call, you expressed disagreement with my statement that I have had to advocate for my ability to work. I would like to provide additional context and evidence on this matter.

On January 4th, I informed HR of my need to go on FMLA. By January 8th, I received the initial copy of the required paperwork (prior to corrections). On January 10th, Rich Hartman notified me that I would not be allowed to work at all, and I began advocating for my ability to continue working in any capacity.

Since the commencement of my FMLA leave, I have consistently advocated for being allowed to perform my job duties. Our current conversations are a continuation of this ongoing effort. If your disagreement stems from a lack of awareness, I hope this message clarifies the situation.

I sincerely hope it will not be necessary to review the extensive communications over the past months, during which my job responsibilities have been reduced or entirely removed. However, I am prepared to do so if required. Any perception that I am unwilling to perform my duties is incorrect. My efforts have always been based on the initial premise that I was not allowed to work at all and had to advocate gradually to take on more responsibilities.

You have been managing the department while I have been continuously advocating for my ability to fulfill my role, piece by piece.

Thank you for your attention to this matter. I am committed to resolving any misunderstandings and ensuring we can move forward collaboratively.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

Exhibit 19D

From:	**Ryan Wagner**
Sent:	**Tuesday, May 21, 2024 3:38 PM**
To:	**Glenn Norris**
Cc:	**Justin Drummond; Rich Hartman; Karen Debus; Matt Norris**
Subject:	**Re: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS**

@Glenn Norris

Thank you for your email. I understand your urgency regarding Ryan Brooks' access and want to ensure we handle this appropriately while maintaining our compliance with PCI DSS 4.0 standards.

1. **Mandates and Requirements:**

   - PFHQ mandates compliance with PCI DSS 4.0, which outlines the specific requirements for all personnel with access to sensitive data and systems. This includes mandatory training and participation in key security processes.

2. **Attestation Filings:**

   - PFHQ instructed me to complete the attestation filings, which are necessary to certify our compliance with PCI DSS 4.0. These filings were submitted to our compliance auditors and relevant regulatory bodies to confirm that we meet all required security standards.

3. **Ryan Brooks' Access:**

   - Restoring Ryan Brooks' access without him completing the required training and participating in mandated security processes would violate our PCI DSS 4.0 compliance. This could jeopardize our certification and the security of our systems.

Could you please clarify the consequences you foresee if we do not restore Ryan's access today? Understanding your concerns will help us address them while ensuring we remain compliant with PCI DSS 4.0 standards.

I must emphasize that compliance with these standards is critical to our operations and security. I am committed to resolving this situation as quickly as possible within the bounds of our compliance requirements.

Please let me know how you would like to proceed, and we can work together to find a solution that maintains our compliance and addresses your needs.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

Exhibit 19D

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093

www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 3:26 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: RE: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

1. Please explain who is mandating this and what it entails.
2. Stop filing attestation filings- who gets these and why were they sent in the last 24 hours?
3. I WANT RYAN'S ACCESS RESTORED TODAY. CONFIRM WHEN THIS IS COMPLETED

Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 2:08 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: Re: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

@Glenn Norris I hope this message finds you well. I appreciate your prompt response regarding Ryan Brooks' compliance and performance. I would like to address the points you raised to ensure clarity and alignment with our compliance requirements and performance expectations.

Compliance Allegations:
Regarding the compliance allegations, it is crucial to clarify that all team members, including vendors, must complete the required PCI DSS compliance training. This is a non-negotiable requirement to maintain our certification and ensure our systems' security and integrity. If Ryan was previously informed that he did not need to complete this training, that was incorrect, and I appreciate his willingness to rectify this.

Exhibit 19D

Compliance Training Requirement:
Ryan must complete the PCI DSS compliance training before he can resume any work, as our attestation has already been filed.
Additional Compliance Requirements:

Beyond the training, Ryan's access has been restricted due to his lack of participation in several PCI DSS-required processes. These include:

Participation in daily standup meetings
Involvement in the change control review board
Engagement in the pipeline for code publishing
Adherence to other necessary procedures
Ryan has previously refused to engage in these processes, which are critical for maintaining our compliance. Additionally, the partial work he has completed has not met PCI DSS compliance standards, and I have had to redo this work to align with our requirements.

Access and Admin Rights:
Regarding your directive to restore Ryan's admin rights immediately, I must emphasize that any such action must comply with our PCI DSS 4 standards. Until Ryan completes the required compliance steps and demonstrates his understanding of PCI DSS requirements, he will not be able to make changes to any system as an administrator. This includes both his software engineer responsibilities and sufficient training for administration.

Next Steps:

Ryan must complete the PCI DSS compliance training immediately.HE IS DOING THIS
Ryan must participate in all PCI DSS required processes, including daily standups, change control review boards, and code publishing pipelines. I DO NOT AGREE
After Ryan completes the training and engages in these processes, we need detailed information on the specific tasks you want him to perform. This will allow us to assign him the least privileged access necessary to maintain PCI compliance.

If you feel it would be helpful, I am open to arranging a meeting with the corporate head of security to weigh in on these items and provide additional perspective on maintaining our compliance and security standards. NO THANK YOU

Thank you for your understanding and cooperation in ensuring we maintain our compliance and security standards. I look forward to resolving this matter collaboratively. I DO NOT AGREE WITH YOUR POSITIONS

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner

Exhibit 19D

Vice President of IT
Ohana Growth Partners, LLC

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 1:48 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>; Glenn Norris <glenn@ohanagp.com>
Subject: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

Ryan, I do not agree with your performance and compliance allegations of Ryan Brooks. I asked him if he was required by you to complete the compliance PCI tests and he was adamant that you stated months ago that he did not need to complete this. He is willing to do it. This is straight from Ryan Brooks.

Regarding his performance, we need to have a conversation on your expectations and role for BC/RB. In my opinion, he has been and still is a valued vendor for our IT needs .

Please ask Justin, Rich, Matt or Karen(and others) how they do or do not value his contribution to our IT needs.

As I stated in our call earlier today, I want his admin rights restored today. There was no discussion with me about this action – I do not approve.

SEE COMMENTS IN RED BELOW

Thank you, Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 1:16 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>
Subject: Ryan Brooks - More Info Needed

Exhibit 19D

@Glenn Norris, I hope you're doing well. I am seeking clarification regarding your directive to retain Ryan Brooks in the IT Department. When we talked today, you expressed a specific need for his services, despite my concerns about his performance and our compliance requirements.

In addition, As part of our compliance with PCI DSS 4 standards, which I recently certified after significant efforts, every team member must meet the requirements. Ryan Brooks' refusal to follow proper procedures and complete the required upskill training posed a substantial obstacle to maintaining PCI DSS 4 unless he is able to do the things that I have required of him.

To clarify:

1. **Security Training**: Ryan has not completed the mandatory security training, which disqualifies him from being employed as a software engineer under PCI DSS 4 standards. HE WILL DO THIS IF IT IS REQUIRED.

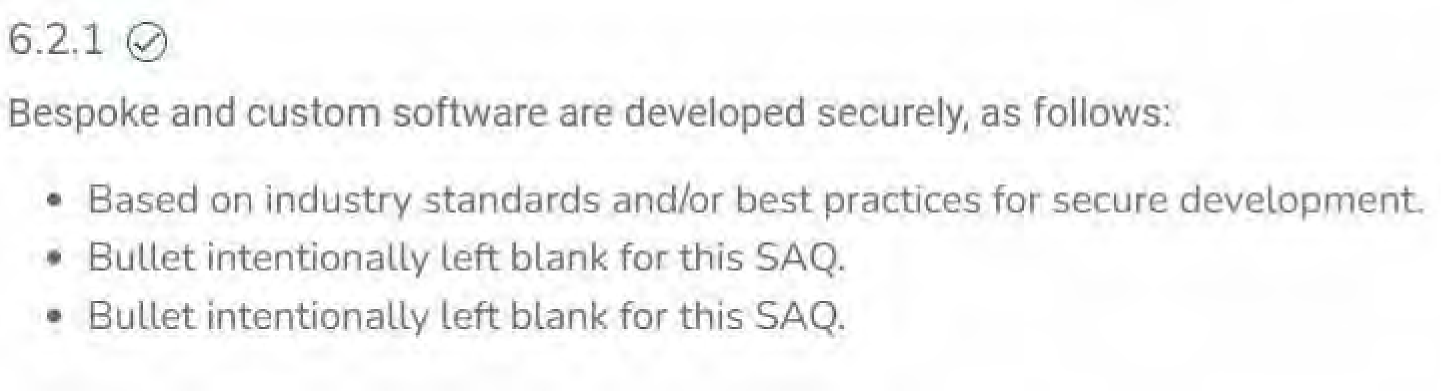
2. **Code Review Process**: He has been unable to participate in the code review process, making him unsuitable for automation or SQL work. WHAT IS THE REQUIRED TIME INVESTMENT HERE?

3. **Change Control Review Board**: Ryan's lack of participation in the change control review board precludes him from performing any sysadmin tasks or handling M365 or Azure responsibilities. HE HAS BEEN ON EVERY TUESDAY 230 CALL AND YOU GHOSTED THAT CALL ON 5-7-24 AND HE WAS IN ATTENDANCE. HE WILL NOT BE ON TODAY'S CALL SINCE YOU INADVERTANTLY FIRED HIM YESTERDAY.

Given these compliance issues, retaining Ryan to work in these areas conflicts with the PCI DSS 4 standards. His non-compliance and refusal to adhere to required protocols undermine our efforts to maintain these critical standards.

Please provide specific details regarding the necessity of retaining Ryan's services and ensure that it does not conflict with our PCI DSS 4 compliance requirements. I would like you to know that understanding your rationale and how it aligns with these standards is essential for moving forward.

Thank you for your attention to this matter. I look forward to your response to resolve this issue in compliance with our obligations.

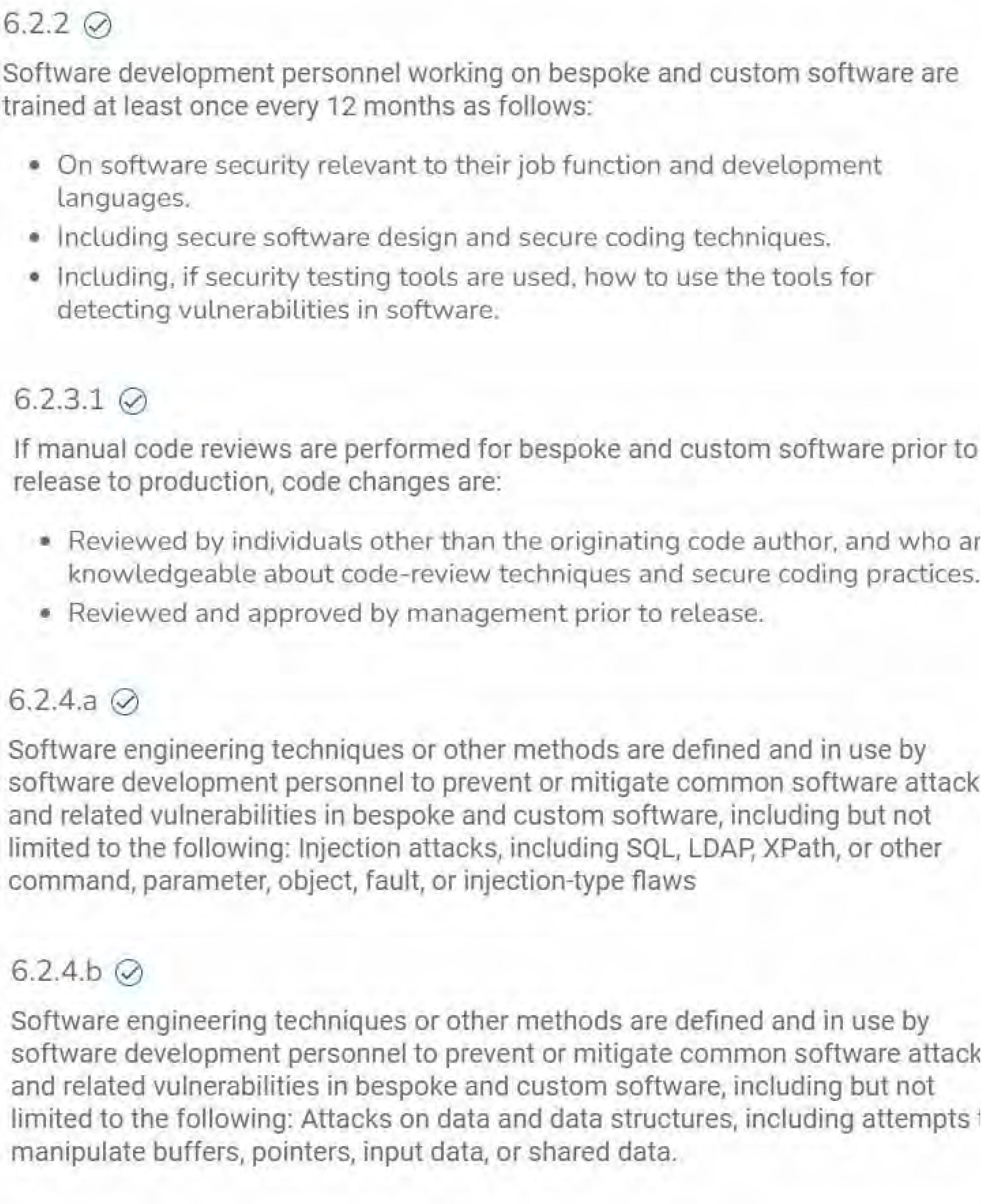


6.2.1 ✓

Bespoke and custom software are developed securely, as follows:

- Based on industry standards and/or best practices for secure development.
- Bullet intentionally left blank for this SAQ.
- Bullet intentionally left blank for this SAQ.

Exhibit 19D



6.2.2 ✓

Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows:

- On software security relevant to their job function and development languages.
- Including secure software design and secure coding techniques.
- Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.

6.2.3.1 ✓

If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are:

- Reviewed by individuals other than the originating code author, and who ar knowledgeable about code-review techniques and secure coding practices.
- Reviewed and approved by management prior to release.

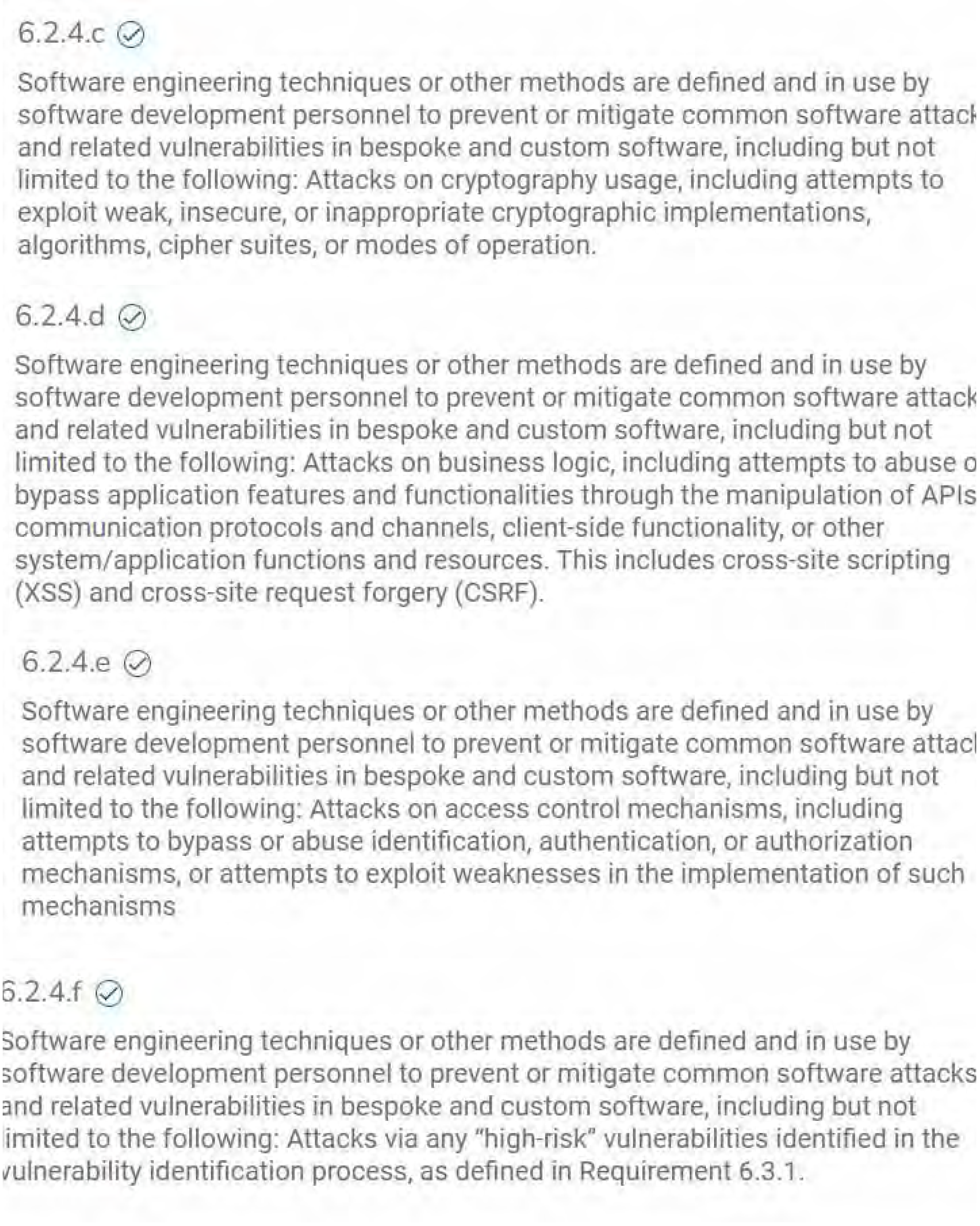
6.2.4.a ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws

6.2.4.b ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on data and data structures, including attempts manipulate buffers, pointers, input data, or shared data.

Exhibit 19D



6.2.4.c ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation.

6.2.4.d ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on business logic, including attempts to abuse o bypass application features and functionalities through the manipulation of APIs communication protocols and channels, client-side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF).

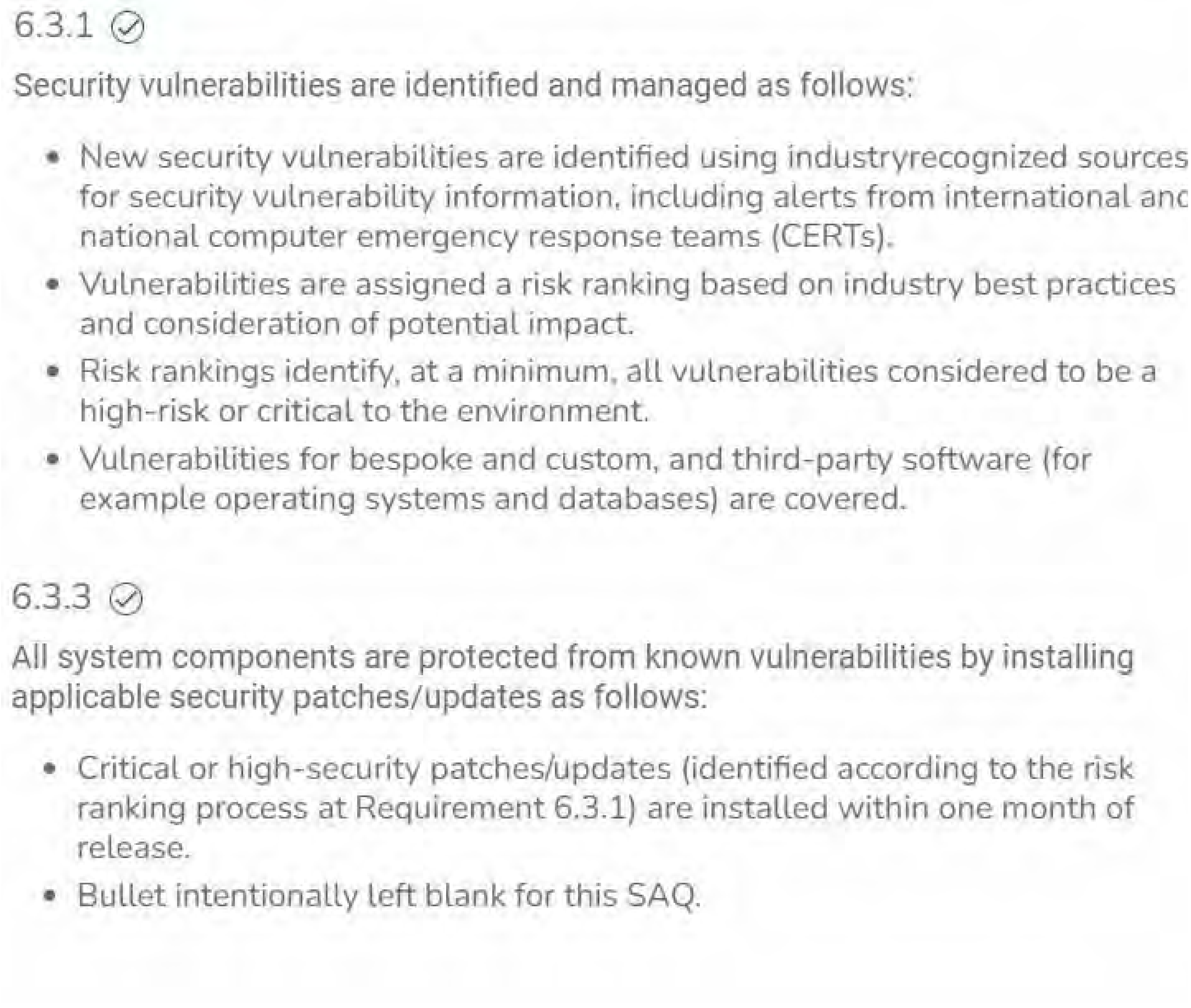
6.2.4.e ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacl and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms

6.2.4.f ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks via any "high-risk" vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1.

Exhibit 19D



6.3.1 ✓

Security vulnerabilities are identified and managed as follows:

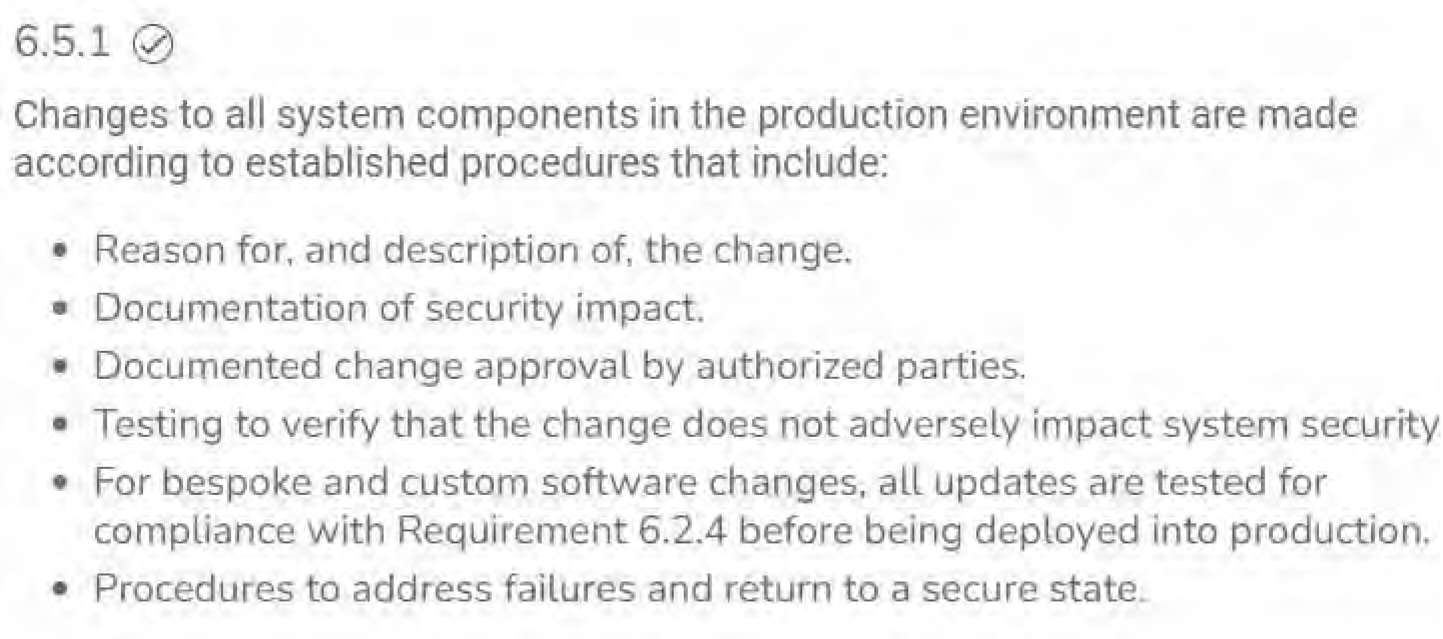
- New security vulnerabilities are identified using industryrecognized sources for security vulnerability information, including alerts from international anc national computer emergency response teams (CERTs).
- Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.
- Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.
- Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.

6.3.3 ✓

All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows:

- Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release.
- Bullet intentionally left blank for this SAQ.

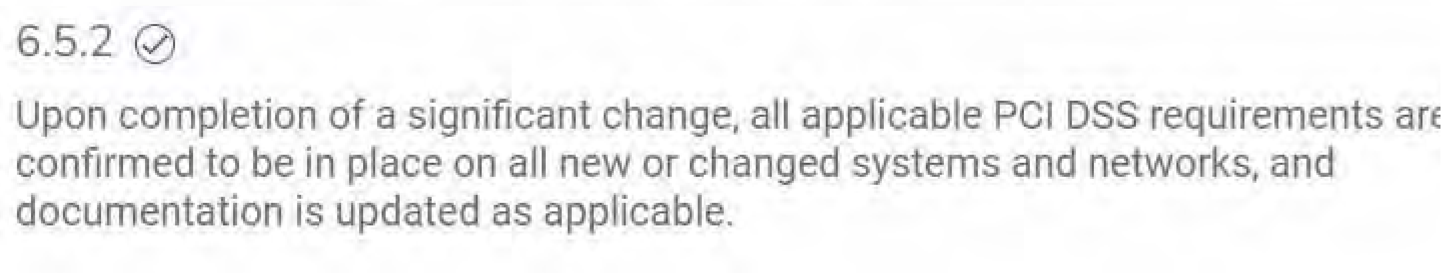
Exhibit 19D



6.5.1 ✓

Changes to all system components in the production environment are made according to established procedures that include:

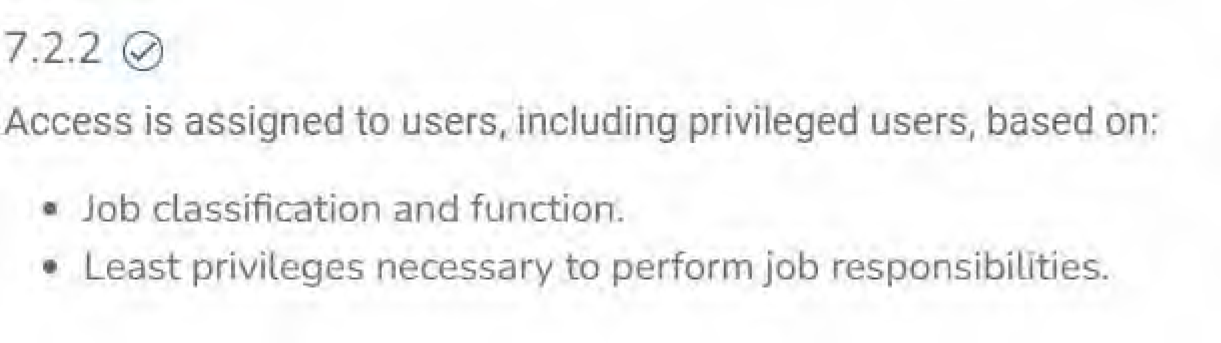
- Reason for, and description of, the change.
- Documentation of security impact.
- Documented change approval by authorized parties.
- Testing to verify that the change does not adversely impact system security
- For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production.
- Procedures to address failures and return to a secure state.



6.5.2 ✓

Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.

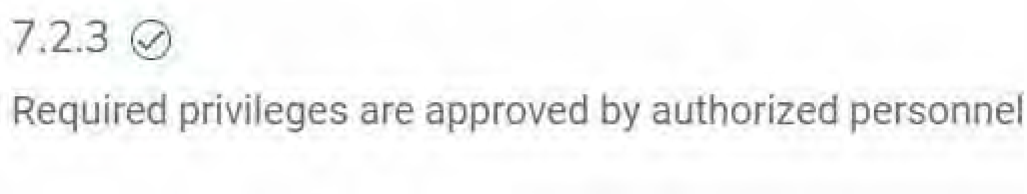
Please provide specific details regarding the necessity of retaining Ryan's services which does not conflict with our PCI DSS 4 compliance requirements. I would like you to know that understanding your rationale and how it aligns with these standards is essential for moving forward by assigning him permissions that will give him the least privileges necessary while not performing tasks listed above or otherwise in the PCI DSS 4.



7.2.2 ✓

Access is assigned to users, including privileged users, based on:

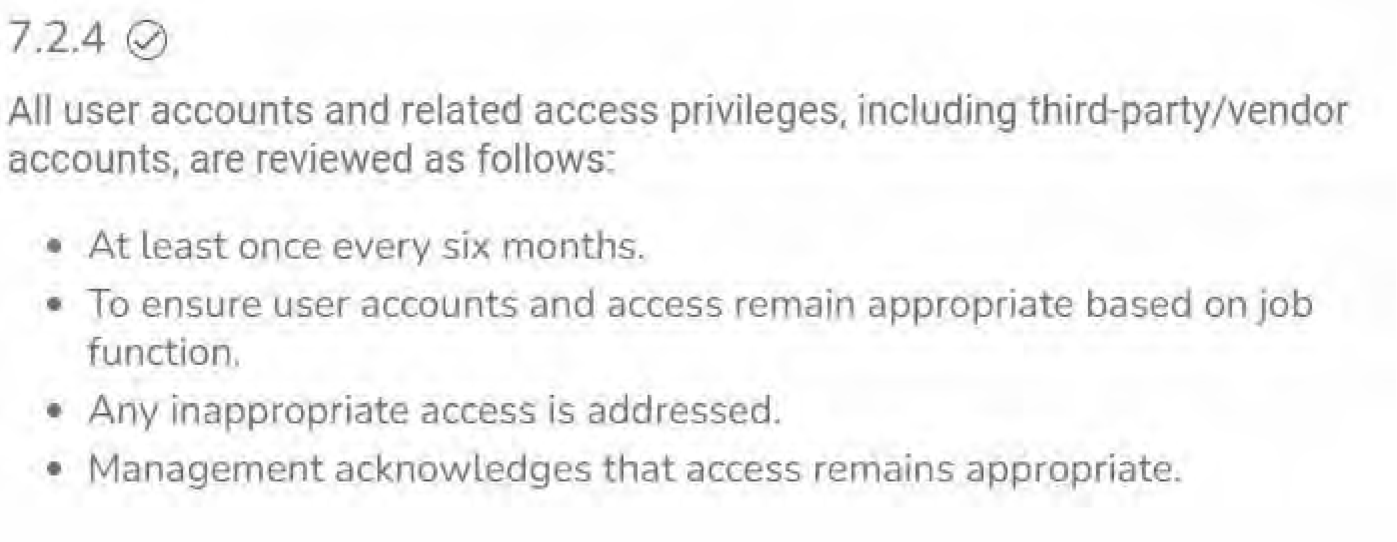
- Job classification and function.
- Least privileges necessary to perform job responsibilities.



7.2.3 ✓

Required privileges are approved by authorized personnel

Exhibit 19D



7.2.4 ✓

All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows:

- At least once every six months.
- To ensure user accounts and access remain appropriate based on job function.
- Any inappropriate access is addressed.
- Management acknowledges that access remains appropriate.

Thank you for your attention to this matter. I look forward to your response and to resolving this issue in accordance with our obligations.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

Exhibit 19E

From:	**Ryan Wagner**
Sent:	**Tuesday, May 21, 2024 4:56 PM**
To:	**Glenn Norris**
Cc:	**Justin Drummond; Rich Hartman; Karen Debus; Matt Norris**
Subject:	**Re: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS**

Thank you for your email. I understand your concerns and would like to clarify the situation regarding Ryan Brooks' access and our compliance requirements.

Compliance and Access Issues:

Yesterday, I consulted with PFHQ about how to handle situations where personnel had not completed required training. Before I could act on the conversation, Ryan Brooks informed me he didn't have time for a mandatory 15-minute meeting, and he had already stated he couldn't complete the required training or other tasks assigned to him. Consequently, I removed him to resolve the block to completing the SAQ, as instructed by PFHQ.

Overnight Changes:

The compliance issues did not change overnight. What changed was the final decision to remove Ryan after he explicitly refused to engage in critical compliance activities. Reinstating his access today would violate PCI DSS 4.0 standards, as I have already informed the head of corporate security that the compliance issue was resolved by terminating his access.

Performance Concerns:

The issues identified by Matt, as well as numerous concerns raised by the accounting department, reflect the quality of Ryan's work. While being responsive is important, it is more critical to ensure that work aligns with our strategic objectives and compliance requirements and does not result in these problems existing. Since September/October, Ryan's recommendations have moved us further from resolution, as evidenced by the ongoing issues highlighted in Matt's email.

Ryan's inability to complete tasks assigned to him and his mismanagement of resources (e.g., setting up a second AVD environment, doubling costs, ignoring Microsoft's recommendations) demonstrate a lack of alignment with our strategic direction. His actions, including making unauthorized changes, have exacerbated our challenges rather than resolving them.

Historical Context:

From the start of the emergency migration project, Ryan proposed outdated solutions, like reinvesting in an old AC system instead of modernizing our platform. Following my HR complaint in November, you stopped supporting the initial proposal and allowed Ryan to make changes against our needs, often in secret. Before my FMLA leave, you reinstated his access despite my concerns. Since FMLA, you and Ryan have been in charge of the IT department. Recently, you informed me I should no longer step back, allowing me to re-establish control and initiate daily standups and other processes to get the team back on track.

Next Steps:

Exhibit 19E

Given the situation:

Ryan must complete the PCI DSS compliance training and participate in the required processes before his access can be reinstated.
Restoring his access without meeting these requirements would jeopardize our PCI DSS 4.0 compliance.
I am committed to resolving these issues in a manner that upholds our compliance standards and addresses our operational needs. Please review the data, recommendations, and conclusions from Microsoft and our current state of issues, which collectively indicate that Ryan is not currently qualified to manage our cloud environment.

We can review these concerns with the head of corporate security, and if I understand why it must happen today, perhaps I can offer a solution that does not result in PCI compliance issues.

Thank you for your understanding and cooperation.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093

www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 4:28 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: RE: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

How was Ryan Brooks allowed access yesterday and not today? What changed overnight, it does not make sense that compliance issues were just discovered and changed overnight.

I do not think your stance flies.

Please do as I have instructed you. He will take the test.

See Matt's reason why we need him. Look at attached email.

Glenn

Glenn Norris

Exhibit 19E

Chief Financial Officer
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 3:38 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: Re: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

@Glenn Norris

Thank you for your email. I understand your urgency regarding Ryan Brooks' access and want to ensure we handle this appropriately while maintaining our compliance with PCI DSS 4.0 standards.

1. **Mandates and Requirements:**

    - PFHQ mandates compliance with PCI DSS 4.0, which outlines the specific requirements for all personnel with access to sensitive data and systems. This includes mandatory training and participation in key security processes.

2. **Attestation Filings:**

    - PFHQ instructed me to complete the attestation filings, which are necessary to certify our compliance with PCI DSS 4.0. These filings were submitted to our compliance auditors and relevant regulatory bodies to confirm that we meet all required security standards.

3. **Ryan Brooks' Access:**

    - Restoring Ryan Brooks' access without him completing the required training and participating in mandated security processes would violate our PCI DSS 4.0 compliance. This could jeopardize our certification and the security of our systems.

Could you please clarify the consequences you foresee if we do not restore Ryan's access today? Understanding your concerns will help us address them while ensuring we remain compliant with PCI DSS 4.0 standards.

I must emphasize that compliance with these standards is critical to our operations and security. I am committed to resolving this situation as quickly as possible within the bounds of our compliance requirements.

Please let me know how you would like to proceed, and we can work together to find a solution that maintains our compliance and addresses your needs.

Exhibit 19E

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

“Culture eats strategy for breakfast”

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 3:26 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: RE: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

1. Please explain who is mandating this and what it entails.
2. Stop filing attestation filings- who gets these and why were they sent in the last 24 hours?
3. I WANT RYAN’S ACCESS RESTORED TODAY. CONFIRM WHEN THIS IS COMPLETED

Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

“Culture eats strategy for breakfast”

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 2:08 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: Re: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

Exhibit 19E

@Glenn Norris I hope this message finds you well. I appreciate your prompt response regarding Ryan Brooks' compliance and performance. I would like to address the points you raised to ensure clarity and alignment with our compliance requirements and performance expectations.

Compliance Allegations:
Regarding the compliance allegations, it is crucial to clarify that all team members, including vendors, must complete the required PCI DSS compliance training. This is a non-negotiable requirement to maintain our certification and ensure our systems' security and integrity. If Ryan was previously informed that he did not need to complete this training, that was incorrect, and I appreciate his willingness to rectify this.

Compliance Training Requirement:
Ryan must complete the PCI DSS compliance training before he can resume any work, as our attestation has already been filed.
Additional Compliance Requirements:

Beyond the training, Ryan's access has been restricted due to his lack of participation in several PCI DSS-required processes. These include:

Participation in daily standup meetings
Involvement in the change control review board
Engagement in the pipeline for code publishing
Adherence to other necessary procedures
Ryan has previously refused to engage in these processes, which are critical for maintaining our compliance. Additionally, the partial work he has completed has not met PCI DSS compliance standards, and I have had to redo this work to align with our requirements.

Access and Admin Rights:
Regarding your directive to restore Ryan's admin rights immediately, I must emphasize that any such action must comply with our PCI DSS 4 standards. Until Ryan completes the required compliance steps and demonstrates his understanding of PCI DSS requirements, he will not be able to make changes to any system as an administrator. This includes both his software engineer responsibilities and sufficient training for administration.

Next Steps:

Ryan must complete the PCI DSS compliance training immediately.HE IS DOING THIS
Ryan must participate in all PCI DSS required processes, including daily standups, change control review boards, and code publishing pipelines. I DO NOT AGREE
After Ryan completes the training and engages in these processes, we need detailed information on the specific tasks you want him to perform. This will allow us to assign him the least privileged access necessary to maintain PCI compliance.

If you feel it would be helpful, I am open to arranging a meeting with the corporate head of security to weigh in on these items and provide additional perspective on maintaining our compliance and security standards. NO THANK YOU

Exhibit 19E

Thank you for your understanding and cooperation in ensuring we maintain our compliance and security standards. I look forward to resolving this matter collaboratively. I DO NOT AGREE WITH YOUR POSITIONS

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 1:48 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>; Glenn Norris <glenn@ohanagp.com>
Subject: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

Ryan, I do not agree with your performance and compliance allegations of Ryan Brooks. I asked him if he was required by you to complete the compliance PCI tests and he was adamant that you stated months ago that he did not need to complete this. He is willing to do it. This is straight from Ryan Brooks.

Regarding his performance, we need to have a conversation on your expectations and role for BC/RB. In my opinion, he has been and still is a valued vendor for our IT needs .

Please ask Justin, Rich, Matt or Karen(and others) how they do or do not value his contribution to our IT needs.

As I stated in our call earlier today, I want his admin rights restored today. There was no discussion with me about this action – I do not approve.

SEE COMMENTS IN RED BELOW

Thank you, Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

Exhibit 19E

OHANA
Growth Partners

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

“Culture eats strategy for breakfast”

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 1:16 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>
Subject: Ryan Brooks - More Info Needed

@Glenn Norris, I hope you're doing well. I am seeking clarification regarding your directive to retain Ryan Brooks in the IT Department. When we talked today, you expressed a specific need for his services, despite my concerns about his performance and our compliance requirements.

In addition, As part of our compliance with PCI DSS 4 standards, which I recently certified after significant efforts, every team member must meet the requirements. Ryan Brooks' refusal to follow proper procedures and complete the required upskill training posed a substantial obstacle to maintaining PCI DSS 4 unless he is able to do the things that I have required of him.

To clarify:

1. **Security Training**: Ryan has not completed the mandatory security training, which disqualifies him from being employed as a software engineer under PCI DSS 4 standards. HE WILL DO THIS IF IT IS REQUIRED.

2. **Code Review Process**: He has been unable to participate in the code review process, making him unsuitable for automation or SQL work. WHAT IS THE REQUIRED TIME INVESTMENT HERE?

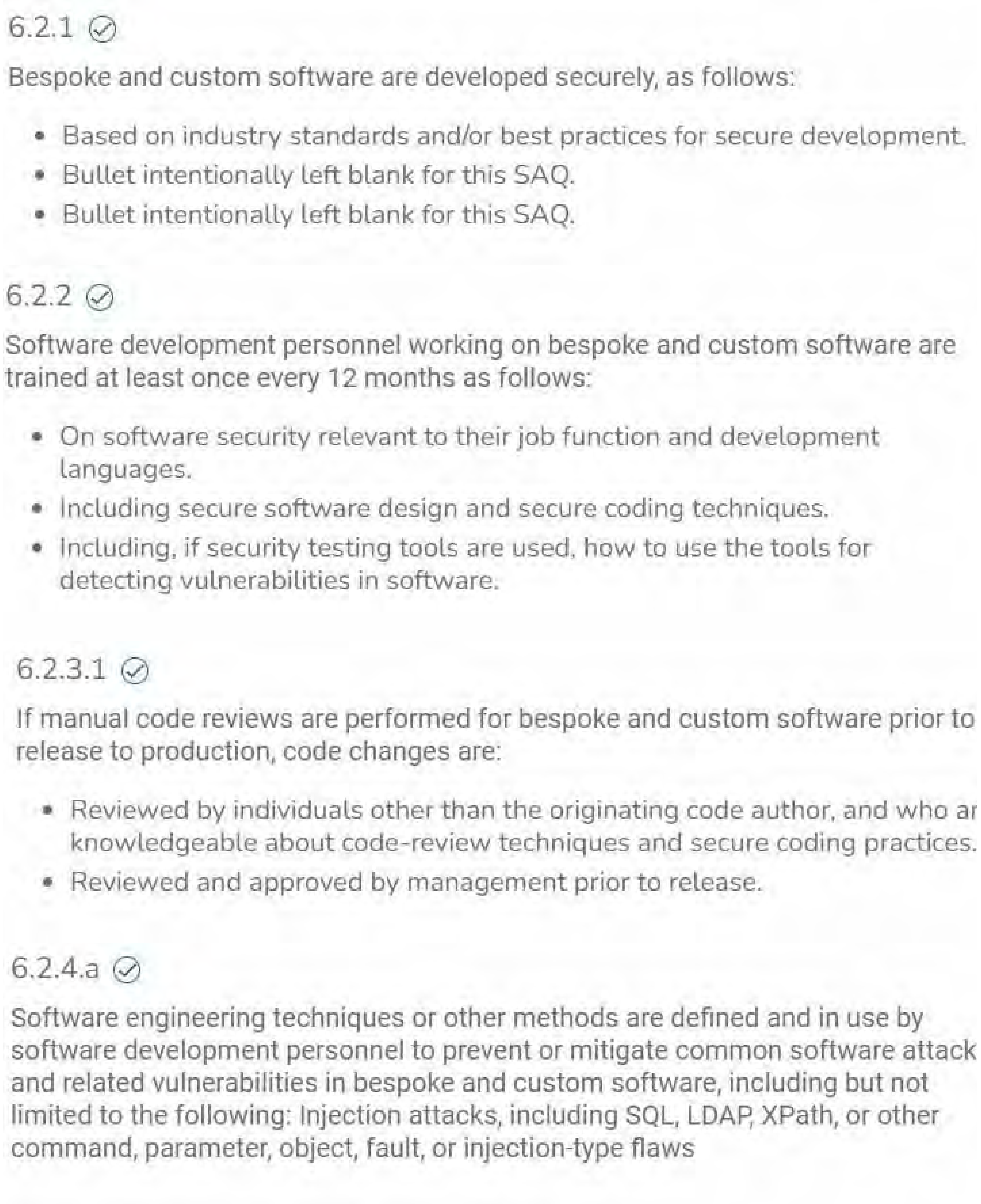
3. **Change Control Review Board**: Ryan's lack of participation in the change control review board precludes him from performing any sysadmin tasks or handling M365 or Azure responsibilities. HE HAS BEEN ON EVERY TUESDAY 230 CALL AND YOU GHOSTED THAT CALL ON 5-7-24 AND HE WAS IN ATTENDANCE. HE WILL NOT BE ON TODAY’S CALL SINCE YOU INADVERTANTLY FIRED HIM YESTERDAY.

Given these compliance issues, retaining Ryan to work in these areas conflicts with the PCI DSS 4 standards. His non-compliance and refusal to adhere to required protocols undermine our efforts to maintain these critical standards.

Please provide specific details regarding the necessity of retaining Ryan's services and ensure that it does not conflict with our PCI DSS 4 compliance requirements. I would like you to know that understanding your rationale and how it aligns with these standards is essential for moving forward.

Thank you for your attention to this matter. I look forward to your response to resolve this issue in compliance with our obligations.

Exhibit 19E



6.2.1 ✓

Bespoke and custom software are developed securely, as follows:

- Based on industry standards and/or best practices for secure development.
- Bullet intentionally left blank for this SAQ.
- Bullet intentionally left blank for this SAQ.

6.2.2 ✓

Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows:

- On software security relevant to their job function and development languages.
- Including secure software design and secure coding techniques.
- Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.

6.2.3.1 ✓

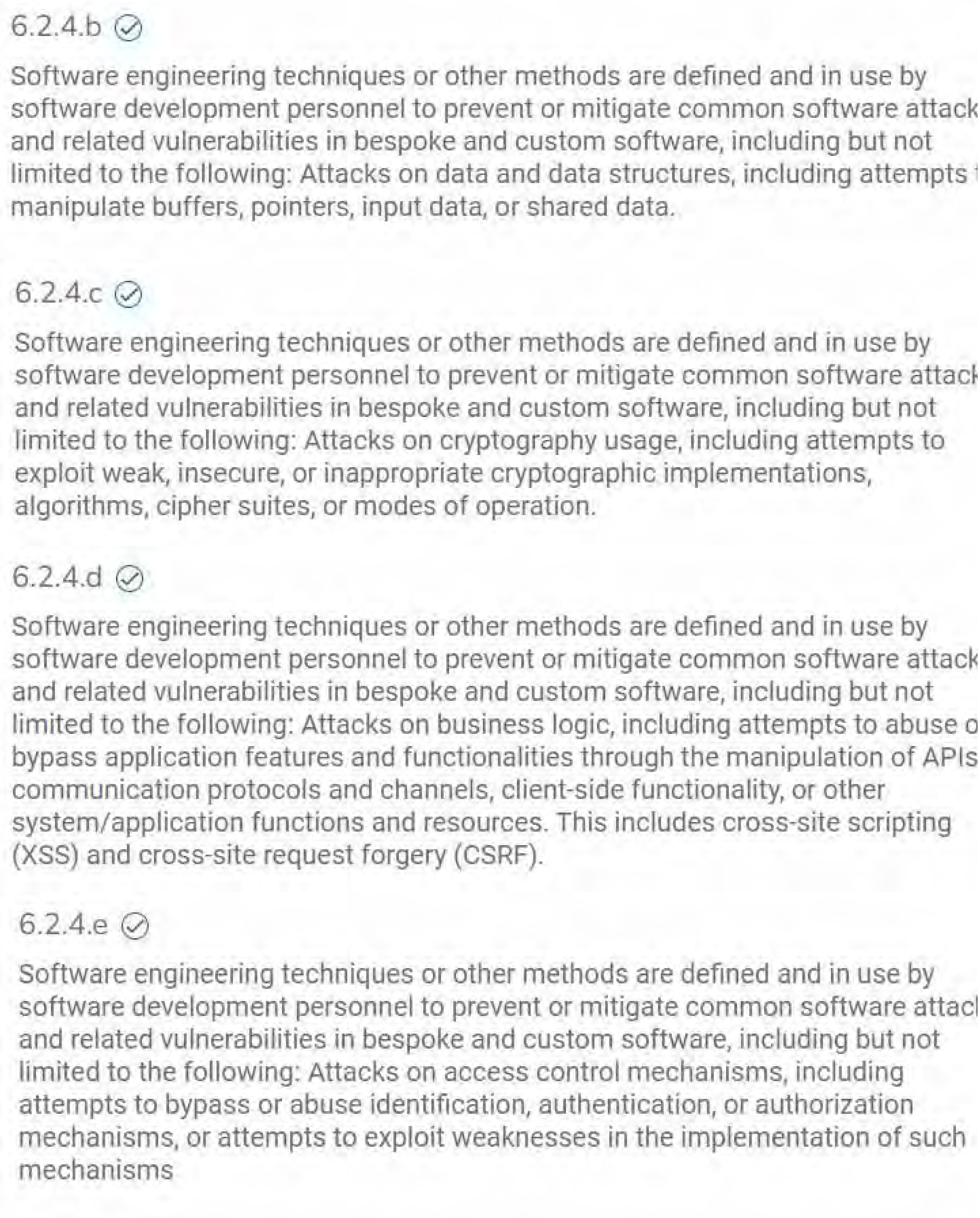
If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are:

- Reviewed by individuals other than the originating code author, and who ar knowledgeable about code-review techniques and secure coding practices.
- Reviewed and approved by management prior to release.

6.2.4.a ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws

Exhibit 19E



6.2.4.b ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on data and data structures, including attempts t manipulate buffers, pointers, input data, or shared data.

6.2.4.c ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation.

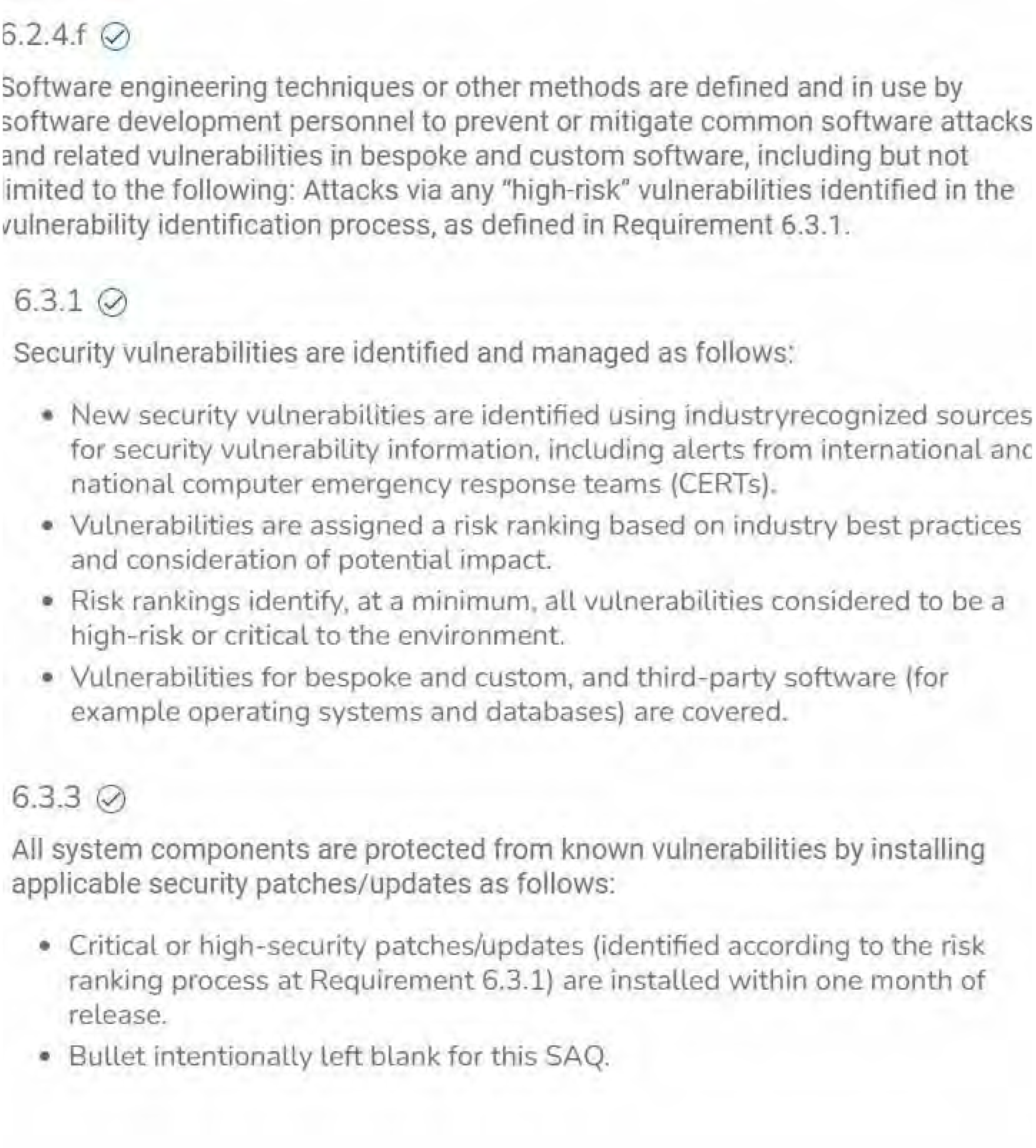
6.2.4.d ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on business logic, including attempts to abuse o bypass application features and functionalities through the manipulation of APIs communication protocols and channels, client-side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF).

6.2.4.e ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms

Exhibit 19E



6.2.4.f ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks via any "high-risk" vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1.

6.3.1 ✓

Security vulnerabilities are identified and managed as follows:

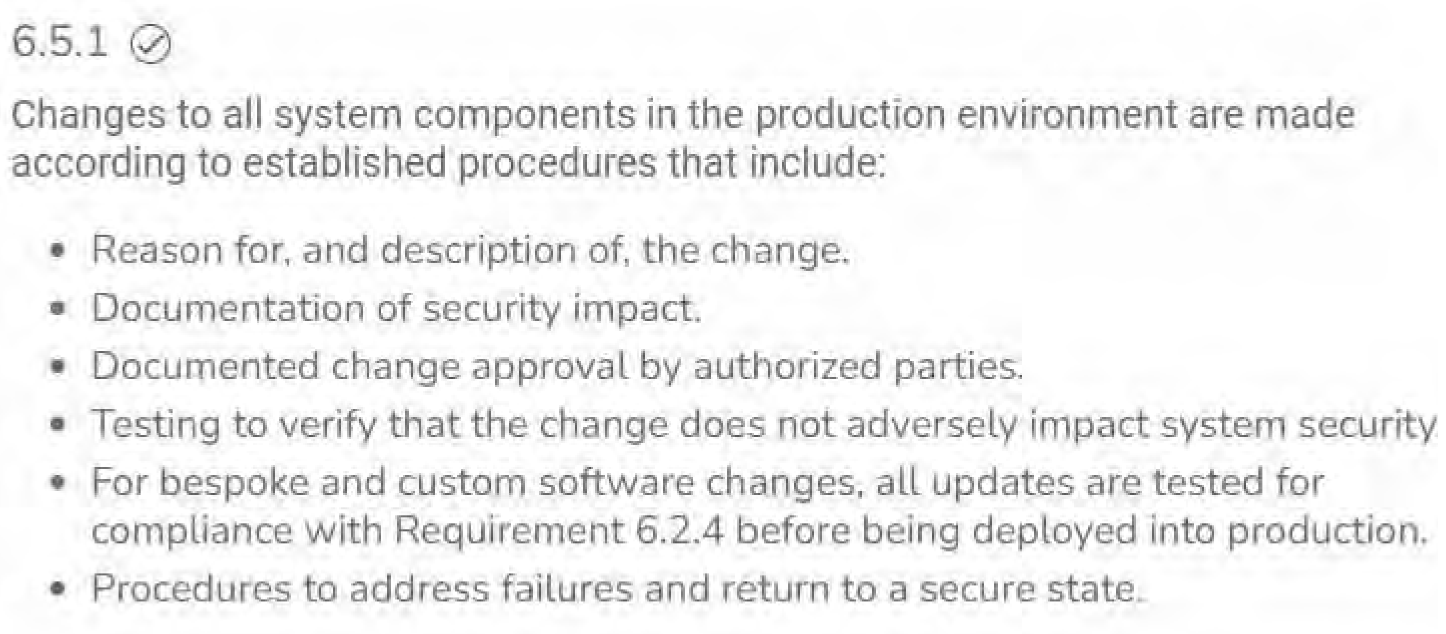
- New security vulnerabilities are identified using industryrecognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).
- Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.
- Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.
- Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.

6.3.3 ✓

All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows:

- Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release.
- Bullet intentionally left blank for this SAQ.

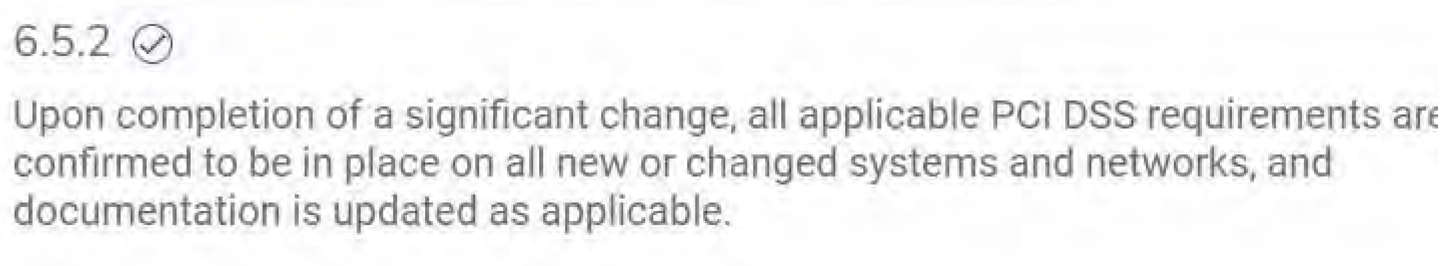
Exhibit 19E



6.5.1 ✓

Changes to all system components in the production environment are made according to established procedures that include:

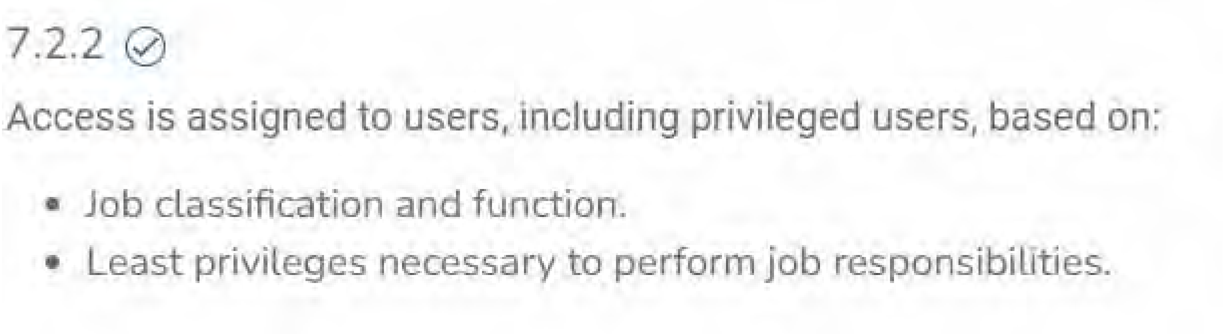
- Reason for, and description of, the change.
- Documentation of security impact.
- Documented change approval by authorized parties.
- Testing to verify that the change does not adversely impact system security
- For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production.
- Procedures to address failures and return to a secure state.



6.5.2 ✓

Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.

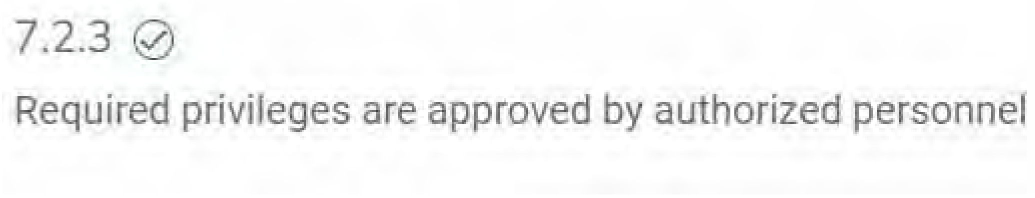
Please provide specific details regarding the necessity of retaining Ryan's services which does not conflict with our PCI DSS 4 compliance requirements. I would like you to know that understanding your rationale and how it aligns with these standards is essential for moving forward by assigning him permissions that will give him the least privileges necessary while not performing tasks listed above or otherwise in the PCI DSS 4.



7.2.2 ✓

Access is assigned to users, including privileged users, based on:

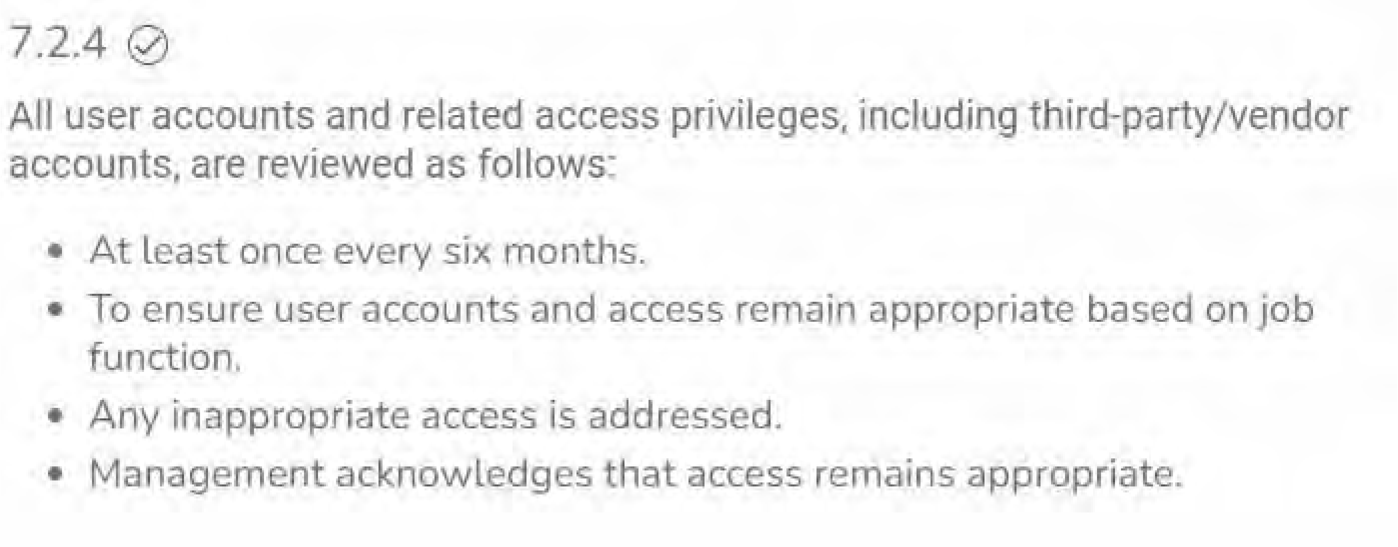
- Job classification and function.
- Least privileges necessary to perform job responsibilities.



7.2.3 ✓

Required privileges are approved by authorized personnel

Exhibit 19E



7.2.4 ✓

All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows:

- At least once every six months.
- To ensure user accounts and access remain appropriate based on job function.
- Any inappropriate access is addressed.
- Management acknowledges that access remains appropriate.

Thank you for your attention to this matter. I look forward to your response and to resolving this issue in accordance with our obligations.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

Exhibit 19F

From:	**Ryan Wagner**
Sent:	**Tuesday, May 21, 2024 5:02 PM**
To:	**Glenn Norris**
Cc:	**Justin Drummond; Rich Hartman; Karen Debus; Matt Norris**
Subject:	**Re: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS**

@Glenn Norris

Thank you for your prompt response. I understand the urgency of your request, but I must reiterate the compliance requirements and potential risks involved in reinstating Ryan Brooks' access without completing the necessary PCI DSS 4.0 training and processes.

Reinstating his access without compliance would put our certification at risk and could have serious legal and security implications for the company. As the head of IT, I have a responsibility to ensure that we adhere to these standards.

Given the gravity of the situation and your directive, I propose a meeting tomorrow morning with you, myself, and the head of corporate security to discuss how we can address this matter without compromising our compliance obligations. This will allow us to find a solution that meets your needs while safeguarding our compliance and security standards.

Please confirm a suitable time for this meeting.

Thank you for your understanding.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093

www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 4:59 PM

Exhibit 19F

To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: RE: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

If Ryan Brooks does not have access by tomorrow morning , you will be written up for insubordination. Is that clear? Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 4:56 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: Re: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

Thank you for your email. I understand your concerns and would like to clarify the situation regarding Ryan Brooks' access and our compliance requirements.

Compliance and Access Issues:

Yesterday, I consulted with PFHQ about how to handle situations where personnel had not completed required training. Before I could act on the conversation, Ryan Brooks informed me he didn't have time for a mandatory 15-minute meeting, and he had already stated he couldn't complete the required training or other tasks assigned to him. Consequently, I removed him to resolve the block to completing the SAQ, as instructed by PFHQ.

Overnight Changes:

The compliance issues did not change overnight. What changed was the final decision to remove Ryan after he explicitly refused to engage in critical compliance activities. Reinstating his access today would violate PCI DSS 4.0 standards, as I have already informed the head of corporate security that the compliance issue was resolved by terminating his access.

Performance Concerns:

The issues identified by Matt, as well as numerous concerns raised by the accounting department, reflect the quality of Ryan's work. While being responsive is important, it is more critical to ensure that work aligns with our strategic objectives and compliance requirements and does not result in these problems existing. Since

Exhibit 19F

September/October, Ryan's recommendations have moved us further from resolution, as evidenced by the ongoing issues highlighted in Matt's email.

Ryan's inability to complete tasks assigned to him and his mismanagement of resources (e.g., setting up a second AVD environment, doubling costs, ignoring Microsoft's recommendations) demonstrate a lack of alignment with our strategic direction. His actions, including making unauthorized changes, have exacerbated our challenges rather than resolving them.

Historical Context:

From the start of the emergency migration project, Ryan proposed outdated solutions, like reinvesting in an old AC system instead of modernizing our platform. Following my HR complaint in November, you stopped supporting the initial proposal and allowed Ryan to make changes against our needs, often in secret. Before my FMLA leave, you reinstated his access despite my concerns. Since FMLA, you and Ryan have been in charge of the IT department. Recently, you informed me I should no longer step back, allowing me to re-establish control and initiate daily standups and other processes to get the team back on track.

Next Steps:

Given the situation:

Ryan must complete the PCI DSS compliance training and participate in the required processes before his access can be reinstated.
Restoring his access without meeting these requirements would jeopardize our PCI DSS 4.0 compliance.
I am committed to resolving these issues in a manner that upholds our compliance standards and addresses our operational needs. Please review the data, recommendations, and conclusions from Microsoft and our current state of issues, which collectively indicate that Ryan is not currently qualified to manage our cloud environment.

We can review these concerns with the head of corporate security, and if I understand why it must happen today, perhaps I can offer a solution that does not result in PCI compliance issues.

Thank you for your understanding and cooperation.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 4:28 PM

Exhibit 19F

To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: RE: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

How was Ryan Brooks allowed access yesterday and not today? What changed overnight, it does not make sense that compliance issues were just discovered and changed overnight.

I do not think your stance flies.

Please do as I have instructed you. He will take the test.

See Matt's reason why we need him. Look at attached email.

Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 3:38 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: Re: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

@Glenn Norris

Thank you for your email. I understand your urgency regarding Ryan Brooks' access and want to ensure we handle this appropriately while maintaining our compliance with PCI DSS 4.0 standards.

1. **Mandates and Requirements:**
   - PFHQ mandates compliance with PCI DSS 4.0, which outlines the specific requirements for all personnel with access to sensitive data and systems. This includes mandatory training and participation in key security processes.
2. **Attestation Filings:**

Exhibit 19F

- PFHQ instructed me to complete the attestation filings, which are necessary to certify our compliance with PCI DSS 4.0. These filings were submitted to our compliance auditors and relevant regulatory bodies to confirm that we meet all required security standards.

3. **Ryan Brooks' Access:**

   - Restoring Ryan Brooks' access without him completing the required training and participating in mandated security processes would violate our PCI DSS 4.0 compliance. This could jeopardize our certification and the security of our systems.

Could you please clarify the consequences you foresee if we do not restore Ryan's access today? Understanding your concerns will help us address them while ensuring we remain compliant with PCI DSS 4.0 standards.

I must emphasize that compliance with these standards is critical to our operations and security. I am committed to resolving this situation as quickly as possible within the bounds of our compliance requirements.

Please let me know how you would like to proceed, and we can work together to find a solution that maintains our compliance and addresses your needs.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 3:26 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: RE: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

1. Please explain who is mandating this and what it entails.
2. Stop filing attestation filings- who gets these and why were they sent in the last 24 hours?
3. I WANT RYAN'S ACCESS RESTORED TODAY. CONFIRM WHEN THIS IS COMPLETED

Glenn

Exhibit 19F

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 2:08 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: Re: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

@Glenn Norris I hope this message finds you well. I appreciate your prompt response regarding Ryan Brooks' compliance and performance. I would like to address the points you raised to ensure clarity and alignment with our compliance requirements and performance expectations.

Compliance Allegations:
Regarding the compliance allegations, it is crucial to clarify that all team members, including vendors, must complete the required PCI DSS compliance training. This is a non-negotiable requirement to maintain our certification and ensure our systems' security and integrity. If Ryan was previously informed that he did not need to complete this training, that was incorrect, and I appreciate his willingness to rectify this.

Compliance Training Requirement:
Ryan must complete the PCI DSS compliance training before he can resume any work, as our attestation has already been filed.
Additional Compliance Requirements:

Beyond the training, Ryan's access has been restricted due to his lack of participation in several PCI DSS-required processes. These include:

Participation in daily standup meetings
Involvement in the change control review board
Engagement in the pipeline for code publishing
Adherence to other necessary procedures
Ryan has previously refused to engage in these processes, which are critical for maintaining our compliance. Additionally, the partial work he has completed has not met PCI DSS compliance standards, and I have had to redo this work to align with our requirements.

Access and Admin Rights:
Regarding your directive to restore Ryan's admin rights immediately, I must emphasize that any such action must comply with our PCI DSS 4 standards. Until Ryan completes the required compliance steps and demonstrates his understanding of PCI DSS requirements, he will not be able to make changes to any system as an administrator. This includes both his software engineer responsibilities and sufficient training for administration.

Next Steps:

Exhibit 19F

Ryan must complete the PCI DSS compliance training immediately.HE IS DOING THIS
Ryan must participate in all PCI DSS required processes, including daily standups, change control review boards, and code publishing pipelines. I DO NOT AGREE
After Ryan completes the training and engages in these processes, we need detailed information on the specific tasks you want him to perform. This will allow us to assign him the least privileged access necessary to maintain PCI compliance.

If you feel it would be helpful, I am open to arranging a meeting with the corporate head of security to weigh in on these items and provide additional perspective on maintaining our compliance and security standards. NO THANK YOU

Thank you for your understanding and cooperation in ensuring we maintain our compliance and security standards. I look forward to resolving this matter collaboratively. I DO NOT AGREE WITH YOUR POSITIONS

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 1:48 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>; Glenn Norris <glenn@ohanagp.com>
Subject: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

Ryan, I do not agree with your performance and compliance allegations of Ryan Brooks. I asked him if he was required by you to complete the compliance PCI tests and he was adamant that you stated months ago that he did not need to complete this. He is willing to do it. This is straight from Ryan Brooks.

Regarding his performance, we need to have a conversation on your expectations and role for BC/RB. In my opinion, he has been and still is a valued vendor for our IT needs .

Exhibit 19F

Please ask Justin, Rich, Matt or Karen(and others) how they do or do not value his contribution to our IT needs.

As I stated in our call earlier today, I want his admin rights restored today. There was no discussion with me about this action – I do not approve.

SEE COMMENTS IN RED BELOW

Thank you, Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 1:16 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>
Subject: Ryan Brooks - More Info Needed

@Glenn Norris, I hope you're doing well. I am seeking clarification regarding your directive to retain Ryan Brooks in the IT Department. When we talked today, you expressed a specific need for his services, despite my concerns about his performance and our compliance requirements.

In addition, As part of our compliance with PCI DSS 4 standards, which I recently certified after significant efforts, every team member must meet the requirements. Ryan Brooks' refusal to follow proper procedures and complete the required upskill training posed a substantial obstacle to maintaining PCI DSS 4 unless he is able to do the things that I have required of him.

To clarify:

1. **Security Training**: Ryan has not completed the mandatory security training, which disqualifies him from being employed as a software engineer under PCI DSS 4 standards. HE WILL DO THIS IF IT IS REQUIRED.

2. **Code Review Process**: He has been unable to participate in the code review process, making him unsuitable for automation or SQL work. WHAT IS THE REQUIRED TIME INVESTMENT HERE?

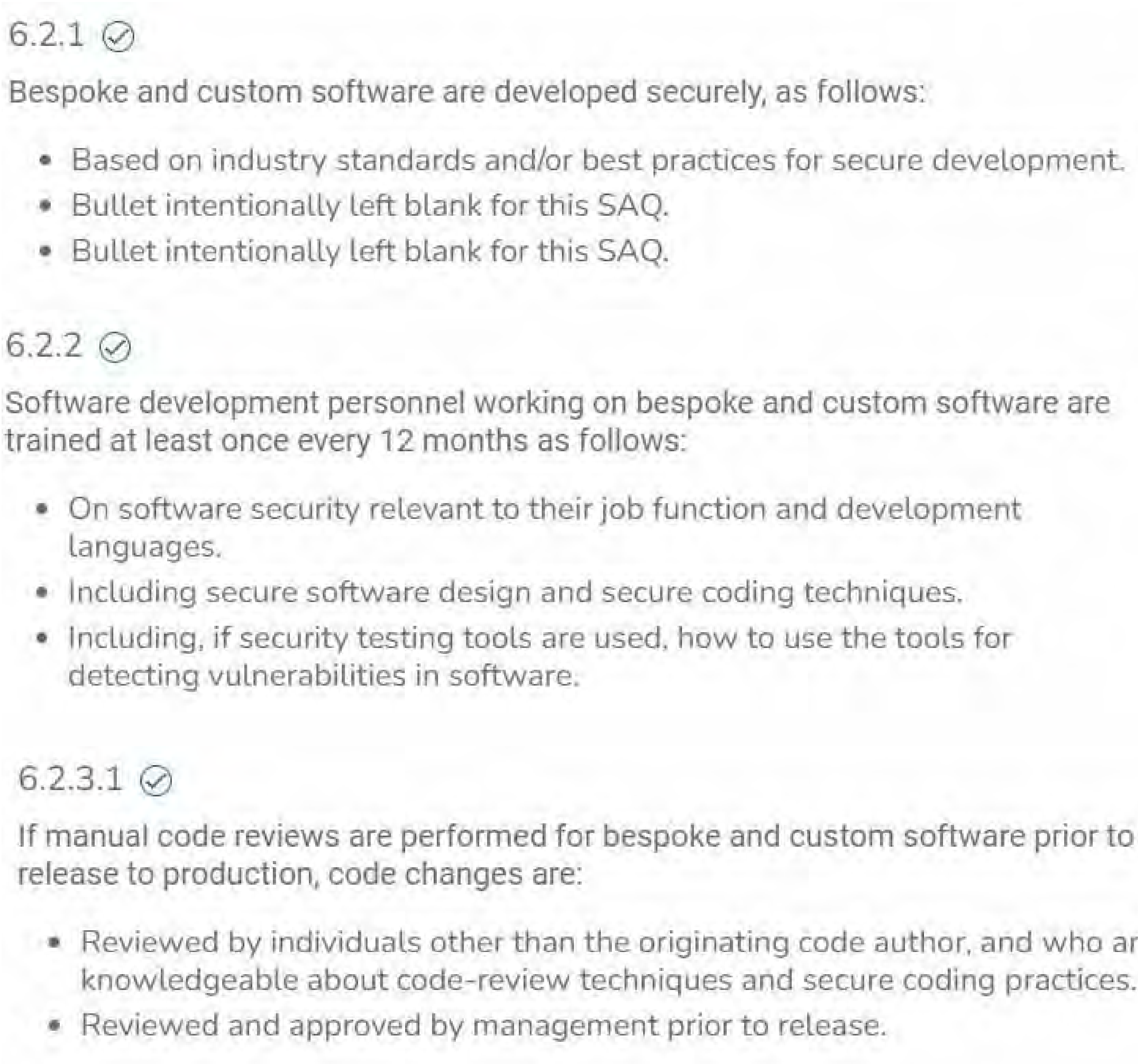
3. **Change Control Review Board**: Ryan's lack of participation in the change control review board precludes him from performing any sysadmin tasks or handling M365 or Azure responsibilities. HE HAS BEEN ON EVERY TUESDAY 230 CALL AND YOU GHOSTED THAT CALL ON 5-7-24 AND HE WAS IN ATTENDANCE. HE WILL NOT BE ON TODAY'S CALL SINCE YOU INADVERTANTLY FIRED HIM YESTERDAY.

Exhibit 19F

Given these compliance issues, retaining Ryan to work in these areas conflicts with the PCI DSS 4 standards. His non-compliance and refusal to adhere to required protocols undermine our efforts to maintain these critical standards.

Please provide specific details regarding the necessity of retaining Ryan's services and ensure that it does not conflict with our PCI DSS 4 compliance requirements. I would like you to know that understanding your rationale and how it aligns with these standards is essential for moving forward.

Thank you for your attention to this matter. I look forward to your response to resolve this issue in compliance with our obligations.



6.2.1 ✓

Bespoke and custom software are developed securely, as follows:

- Based on industry standards and/or best practices for secure development.
- Bullet intentionally left blank for this SAQ.
- Bullet intentionally left blank for this SAQ.

6.2.2 ✓

Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows:

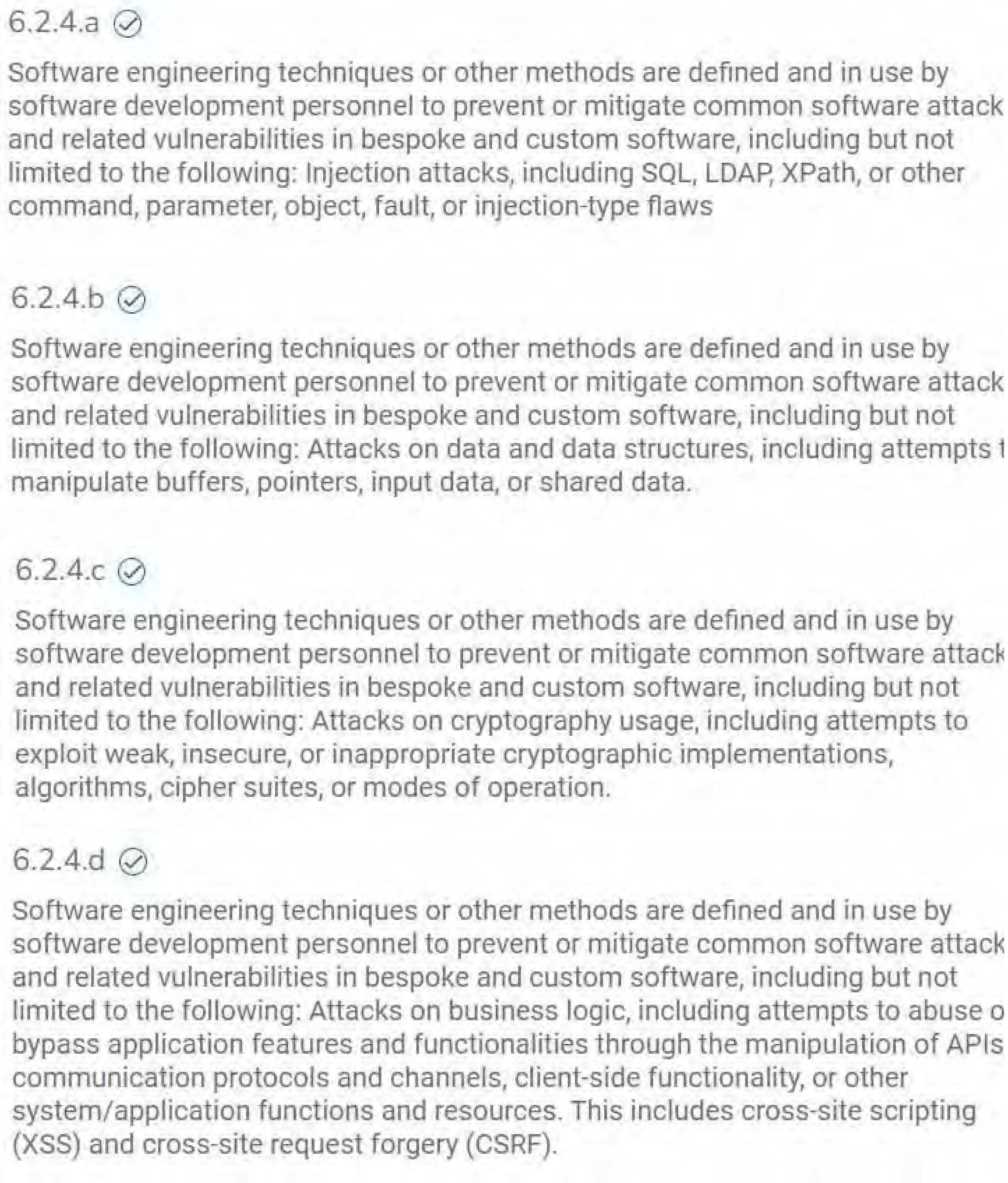
- On software security relevant to their job function and development languages.
- Including secure software design and secure coding techniques.
- Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.

6.2.3.1 ✓

If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are:

- Reviewed by individuals other than the originating code author, and who ar knowledgeable about code-review techniques and secure coding practices.
- Reviewed and approved by management prior to release.

Exhibit 19F



6.2.4.a ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws

6.2.4.b ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on data and data structures, including attempts t manipulate buffers, pointers, input data, or shared data.

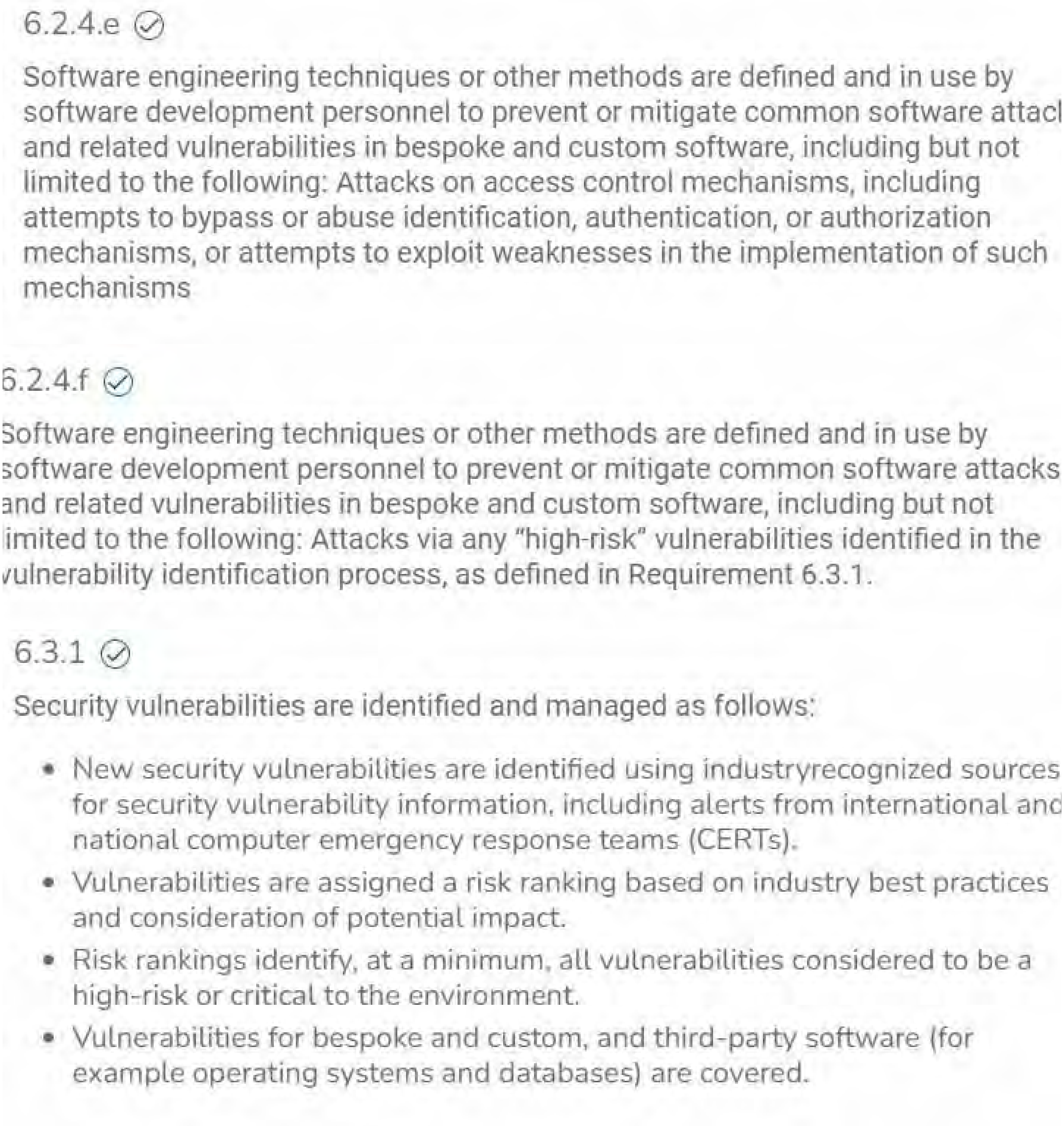
6.2.4.c ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation.

6.2.4.d ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on business logic, including attempts to abuse o bypass application features and functionalities through the manipulation of APIs communication protocols and channels, client-side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF).

Exhibit 19F



6.2.4.e ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacl and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms

6.2.4.f ✓

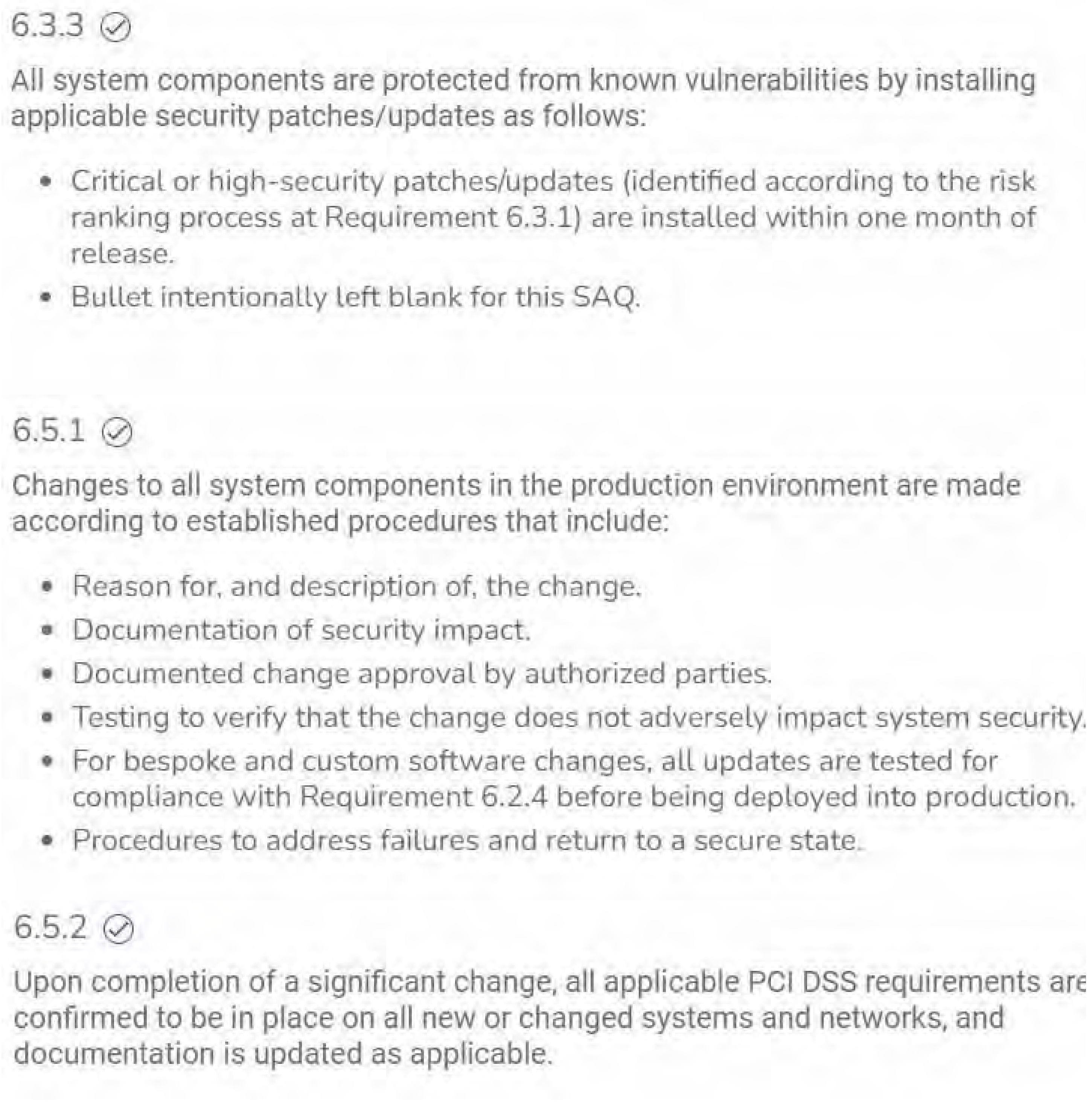
Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks via any "high-risk" vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1.

6.3.1 ✓

Security vulnerabilities are identified and managed as follows:

- New security vulnerabilities are identified using industryrecognized sources for security vulnerability information, including alerts from international anc national computer emergency response teams (CERTs).
- Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.
- Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.
- Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.

Exhibit 19F



6.3.3 ✓

All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows:

- Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release.
- Bullet intentionally left blank for this SAQ.

6.5.1 ✓

Changes to all system components in the production environment are made according to established procedures that include:

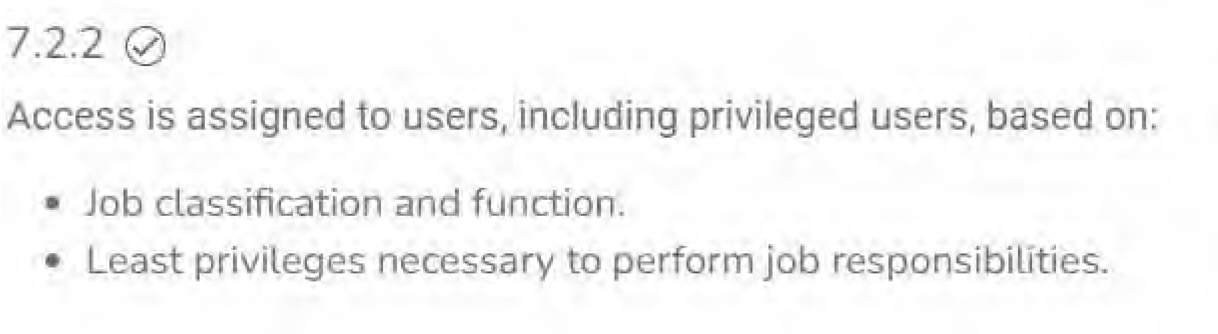
- Reason for, and description of, the change.
- Documentation of security impact.
- Documented change approval by authorized parties.
- Testing to verify that the change does not adversely impact system security.
- For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production.
- Procedures to address failures and return to a secure state.

6.5.2 ✓

Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.

Please provide specific details regarding the necessity of retaining Ryan's services which does not conflict with our PCI DSS 4 compliance requirements. I would like you to know that understanding your rationale and how it aligns with these standards is essential for moving forward by assigning him permissions that will give him the least privileges necessary while not performing tasks listed above or otherwise in the PCI DSS 4.

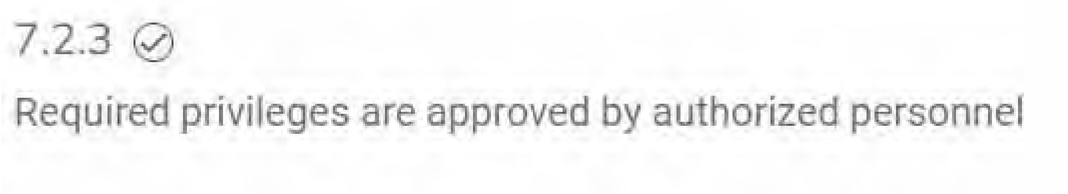
Exhibit 19F



7.2.2 ✓

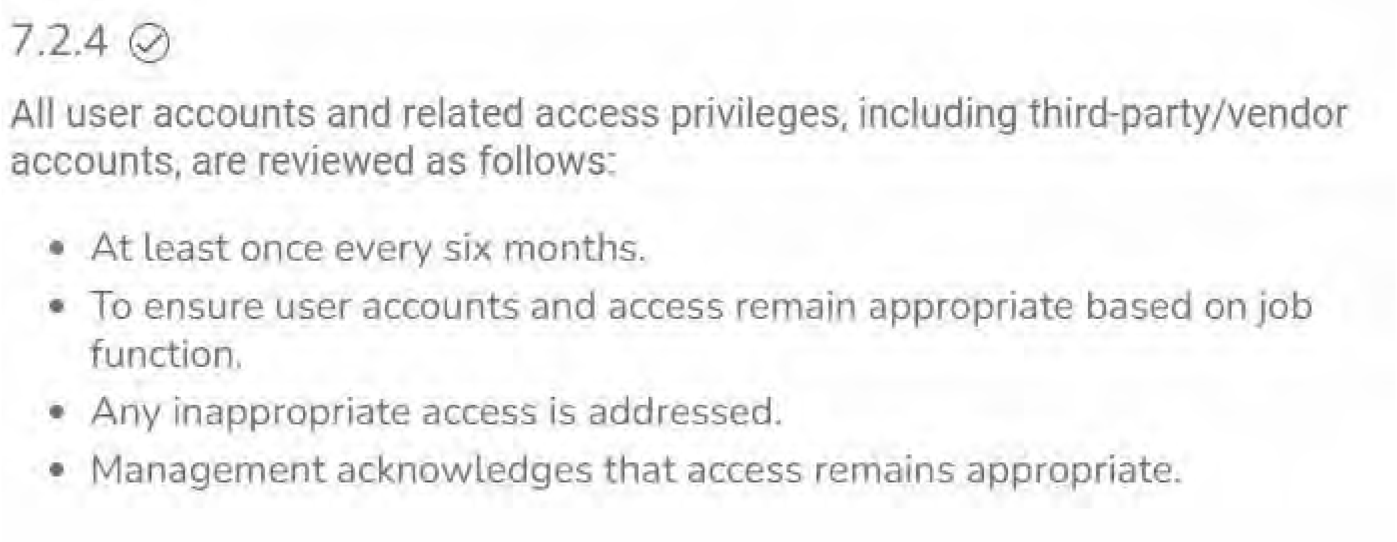
Access is assigned to users, including privileged users, based on:

- Job classification and function.
- Least privileges necessary to perform job responsibilities.



7.2.3 ✓

Required privileges are approved by authorized personnel



7.2.4 ✓

All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows:

- At least once every six months.
- To ensure user accounts and access remain appropriate based on job function.
- Any inappropriate access is addressed.
- Management acknowledges that access remains appropriate.

Thank you for your attention to this matter. I look forward to your response and to resolving this issue in accordance with our obligations.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

Exhibit 19F

OHANA
Growth Partners

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

Exhibit 19G

From:	**Ryan Wagner**
Sent:	**Tuesday, May 21, 2024 5:10 PM**
To:	**Geoff VanMaastricht; Glenn Norris**
Cc:	**Justin Drummond**
Subject:	**SAQ - PCI Compliance : We need your assistance**

@Geoff VanMaastricht , Would you be available for a meeting tomorrow to discuss this and related PCI Compliance concerns? I am being told to reinstate the same person, but they refuse to do the training, take part in the code review, change control, or any other process to maintain compliance. I don't know what to do and could use your assistance to find a solution that works for our CFO as well as meet the compliance

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093

www.planetfitness.com

"Culture eats strategy for breakfast"

Exhibit 19H

From:	**Ryan Wagner**
Sent:	**Tuesday, May 21, 2024 5:13 PM**
To:	**Glenn Norris**
Cc:	**Justin Drummond; Rich Hartman; Karen Debus; Matt Norris**
Subject:	**Re: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS**

I acknowledge your directive and understand the urgency of the situation. However, I must reiterate the compliance risks associated with reinstating Ryan Brooks' access without him completing the necessary PCI DSS 4.0 training and processes.

As the head of IT, my primary responsibility is to ensure that we maintain compliance with all regulatory standards. Restoring Ryan's access without meeting these requirements places our PCI DSS 4.0 certification and the company at significant risk. While I am prepared to follow your instructions, I must stress that this action is being undertaken under duress due to your explicit directive.

I have reached out to Geoff VanMaastricht, our head of corporate security, to seek his assistance in finding a solution that balances our compliance obligations with your request. Here is the email I sent to him, which includes you and President Justin Drummond in the loop:

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093

www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner Ryan.Wagner@ohanagp.com
Sent: Tuesday, May 21, 2024 5:09 PM
To: Geoff VanMaastricht Geoff.VanMaastricht@pfhq.com
Cc: Glenn Norris glenn@ohanagp.com; Justin Drummond Justin.Drummond@ohanagp.com
Subject: SAQ - PCI Compliance: We need your assistance

@Geoff VanMaastricht, Would you be available for a meeting tomorrow to discuss this and related PCI Compliance concerns? I am being told to reinstate the same person, but they refuse to do the training, take part in the code review, change control, or any other process to maintain compliance. I don't know what to do and could use your assistance to find a solution that works for our CFO as well as meet the compliance requirements.

To mitigate these risks and protect our compliance standing, I propose the following steps:

Immediate Compliance Training: Expedite Ryan's PCI DSS 4.0 compliance training and ensure it is completed as a top priority.
Temporary Limited Access: Provide Ryan with limited access necessary for immediate tasks, under close monitoring, until he completes the required training and processes.

Exhibit 19H

Documented Agreement: Document this course of action, including the acknowledgment that this decision is made under duress, to protect both the company and ourselves, ensuring we have a record of our compliance efforts and the rationale behind these decisions.
I am available to discuss this further and facilitate any immediate actions required to address your concerns while maintaining our compliance obligations.

Please let me know how you would like to proceed.

Best regards,

This message may include text created with the help of natural language processing.

Book time to meet with me

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 5:05 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: RE: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

Rich, please prepare a write up for me .

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 5:02 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: Re: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

@Glenn Norris

Thank you for your prompt response. I understand the urgency of your request, but I must reiterate the compliance requirements and potential risks involved in reinstating Ryan Brooks' access without completing the necessary PCI DSS 4.0 training and processes.

Exhibit 19H

Reinstating his access without compliance would put our certification at risk and could have serious legal and security implications for the company. As the head of IT, I have a responsibility to ensure that we adhere to these standards.

Given the gravity of the situation and your directive, I propose a meeting tomorrow morning with you, myself, and the head of corporate security to discuss how we can address this matter without compromising our compliance obligations. This will allow us to find a solution that meets your needs while safeguarding our compliance and security standards.

Please confirm a suitable time for this meeting.

Thank you for your understanding.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 4:59 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: RE: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

If Ryan Brooks does not have access by tomorrow morning , you will be written up for insubordination. Is that clear? Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

Exhibit 19H

OHANA
Growth Partners

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 4:56 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: Re: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

Thank you for your email. I understand your concerns and would like to clarify the situation regarding Ryan Brooks' access and our compliance requirements.

Compliance and Access Issues:

Yesterday, I consulted with PFHQ about how to handle situations where personnel had not completed required training. Before I could act on the conversation, Ryan Brooks informed me he didn't have time for a mandatory 15-minute meeting, and he had already stated he couldn't complete the required training or other tasks assigned to him. Consequently, I removed him to resolve the block to completing the SAQ, as instructed by PFHQ.

Overnight Changes:

The compliance issues did not change overnight. What changed was the final decision to remove Ryan after he explicitly refused to engage in critical compliance activities. Reinstating his access today would violate PCI DSS 4.0 standards, as I have already informed the head of corporate security that the compliance issue was resolved by terminating his access.

Performance Concerns:

The issues identified by Matt, as well as numerous concerns raised by the accounting department, reflect the quality of Ryan's work. While being responsive is important, it is more critical to ensure that work aligns with our strategic objectives and compliance requirements and does not result in these problems existing. Since September/October, Ryan's recommendations have moved us further from resolution, as evidenced by the ongoing issues highlighted in Matt's email.

Ryan's inability to complete tasks assigned to him and his mismanagement of resources (e.g., setting up a second AVD environment, doubling costs, ignoring Microsoft's recommendations) demonstrate a lack of alignment with our strategic direction. His actions, including making unauthorized changes, have exacerbated our challenges rather than resolving them.

Historical Context:

From the start of the emergency migration project, Ryan proposed outdated solutions, like reinvesting in an old AC system instead of modernizing our platform. Following my HR complaint in November, you stopped supporting the initial proposal and allowed Ryan to make changes against our needs, often in secret. Before my FMLA leave, you

Exhibit 19H

reinstated his access despite my concerns. Since FMLA, you and Ryan have been in charge of the IT department. Recently, you informed me I should no longer step back, allowing me to re-establish control and initiate daily standups and other processes to get the team back on track.

Next Steps:

Given the situation:

Ryan must complete the PCI DSS compliance training and participate in the required processes before his access can be reinstated.
Restoring his access without meeting these requirements would jeopardize our PCI DSS 4.0 compliance.
I am committed to resolving these issues in a manner that upholds our compliance standards and addresses our operational needs. Please review the data, recommendations, and conclusions from Microsoft and our current state of issues, which collectively indicate that Ryan is not currently qualified to manage our cloud environment.

We can review these concerns with the head of corporate security, and if I understand why it must happen today, perhaps I can offer a solution that does not result in PCI compliance issues.

Thank you for your understanding and cooperation.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 4:28 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: RE: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

How was Ryan Brooks allowed access yesterday and not today? What changed overnight, it does not make sense that compliance issues were just discovered and changed overnight.

I do not think your stance flies.

Please do as I have instructed you. He will take the test.

See Matt's reason why we need him. Look at attached email.

Exhibit 19H

Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 3:38 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: Re: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

@Glenn Norris

Thank you for your email. I understand your urgency regarding Ryan Brooks' access and want to ensure we handle this appropriately while maintaining our compliance with PCI DSS 4.0 standards.

1. **Mandates and Requirements:**

   - PFHQ mandates compliance with PCI DSS 4.0, which outlines the specific requirements for all personnel with access to sensitive data and systems. This includes mandatory training and participation in key security processes.

2. **Attestation Filings:**

   - PFHQ instructed me to complete the attestation filings, which are necessary to certify our compliance with PCI DSS 4.0. These filings were submitted to our compliance auditors and relevant regulatory bodies to confirm that we meet all required security standards.

3. **Ryan Brooks' Access:**

   - Restoring Ryan Brooks' access without him completing the required training and participating in mandated security processes would violate our PCI DSS 4.0 compliance. This could jeopardize our certification and the security of our systems.

Could you please clarify the consequences you foresee if we do not restore Ryan's access today? Understanding your concerns will help us address them while ensuring we remain compliant with PCI DSS 4.0 standards.

I must emphasize that compliance with these standards is critical to our operations and security. I am committed to resolving this situation as quickly as possible within the bounds of our compliance requirements.

Exhibit 19H

Please let me know how you would like to proceed, and we can work together to find a solution that maintains our compliance and addresses your needs.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 3:26 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: RE: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

1. Please explain who is mandating this and what it entails.
2. Stop filing attestation filings- who gets these and why were they sent in the last 24 hours?
3. I WANT RYAN'S ACCESS RESTORED TODAY. CONFIRM WHEN THIS IS COMPLETED

Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 2:08 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus

Exhibit 19H

<karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: Re: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

@Glenn Norris I hope this message finds you well. I appreciate your prompt response regarding Ryan Brooks' compliance and performance. I would like to address the points you raised to ensure clarity and alignment with our compliance requirements and performance expectations.

Compliance Allegations:
Regarding the compliance allegations, it is crucial to clarify that all team members, including vendors, must complete the required PCI DSS compliance training. This is a non-negotiable requirement to maintain our certification and ensure our systems' security and integrity. If Ryan was previously informed that he did not need to complete this training, that was incorrect, and I appreciate his willingness to rectify this.

Compliance Training Requirement:
Ryan must complete the PCI DSS compliance training before he can resume any work, as our attestation has already been filed.
Additional Compliance Requirements:

Beyond the training, Ryan's access has been restricted due to his lack of participation in several PCI DSS-required processes. These include:

Participation in daily standup meetings
Involvement in the change control review board
Engagement in the pipeline for code publishing
Adherence to other necessary procedures
Ryan has previously refused to engage in these processes, which are critical for maintaining our compliance. Additionally, the partial work he has completed has not met PCI DSS compliance standards, and I have had to redo this work to align with our requirements.

Access and Admin Rights:
Regarding your directive to restore Ryan's admin rights immediately, I must emphasize that any such action must comply with our PCI DSS 4 standards. Until Ryan completes the required compliance steps and demonstrates his understanding of PCI DSS requirements, he will not be able to make changes to any system as an administrator. This includes both his software engineer responsibilities and sufficient training for administration.

Next Steps:

Ryan must complete the PCI DSS compliance training immediately.HE IS DOING THIS
Ryan must participate in all PCI DSS required processes, including daily standups, change control review boards, and code publishing pipelines. I DO NOT AGREE
After Ryan completes the training and engages in these processes, we need detailed information on the specific tasks you want him to perform. This will allow us to assign him the least privileged access necessary to maintain PCI compliance.

If you feel it would be helpful, I am open to arranging a meeting with the corporate head of security to weigh in on these items and provide additional perspective on

Exhibit 19H

maintaining our compliance and security standards. NO THANK YOU

Thank you for your understanding and cooperation in ensuring we maintain our compliance and security standards. I look forward to resolving this matter collaboratively. I DO NOT AGREE WITH YOUR POSITIONS

This message may include text created with the help of natural language processing.

[Book time to meet with me]

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 1:48 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>; Glenn Norris <glenn@ohanagp.com>
Subject: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

Ryan, I do not agree with your performance and compliance allegations of Ryan Brooks. I asked him if he was required by you to complete the compliance PCI tests and he was adamant that you stated months ago that he did not need to complete this. He is willing to do it. This is straight from Ryan Brooks.

Regarding his performance, we need to have a conversation on your expectations and role for BC/RB. In my opinion, he has been and still is a valued vendor for our IT needs .

Please ask Justin, Rich, Matt or Karen(and others) how they do or do not value his contribution to our IT needs.

As I stated in our call earlier today, I want his admin rights restored today. There was no discussion with me about this action – I do not approve.

SEE COMMENTS IN RED BELOW

Thank you, Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

Exhibit 19H

OHANA
Growth Partners

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 1:16 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>
Subject: Ryan Brooks - More Info Needed

@Glenn Norris, I hope you're doing well. I am seeking clarification regarding your directive to retain Ryan Brooks in the IT Department. When we talked today, you expressed a specific need for his services, despite my concerns about his performance and our compliance requirements.

In addition, As part of our compliance with PCI DSS 4 standards, which I recently certified after significant efforts, every team member must meet the requirements. Ryan Brooks' refusal to follow proper procedures and complete the required upskill training posed a substantial obstacle to maintaining PCI DSS 4 unless he is able to do the things that I have required of him.

To clarify:

1. **Security Training**: Ryan has not completed the mandatory security training, which disqualifies him from being employed as a software engineer under PCI DSS 4 standards. HE WILL DO THIS IF IT IS REQUIRED.

2. **Code Review Process**: He has been unable to participate in the code review process, making him unsuitable for automation or SQL work. WHAT IS THE REQUIRED TIME INVESTMENT HERE?

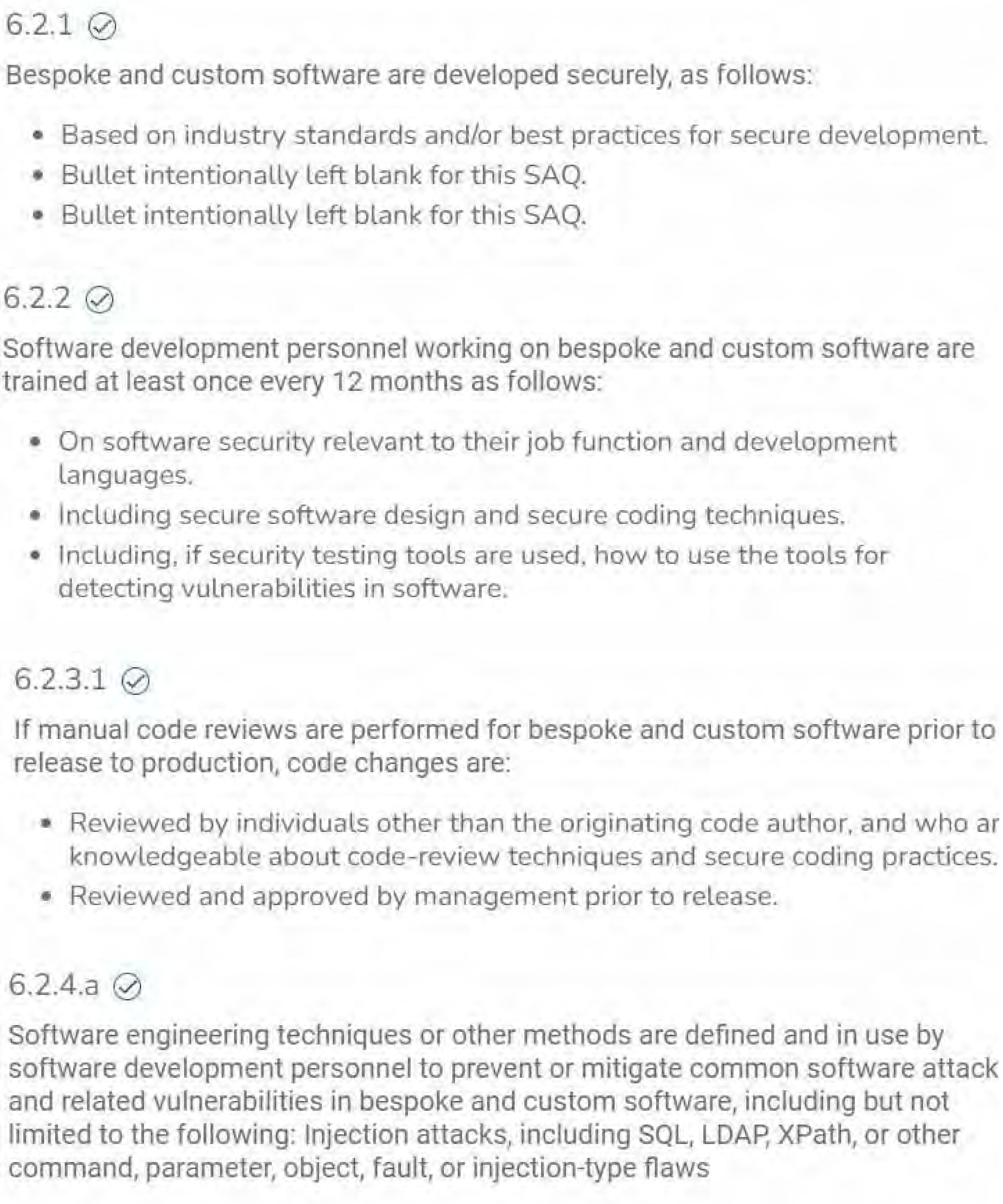
3. **Change Control Review Board**: Ryan's lack of participation in the change control review board precludes him from performing any sysadmin tasks or handling M365 or Azure responsibilities. HE HAS BEEN ON EVERY TUESDAY 230 CALL AND YOU GHOSTED THAT CALL ON 5-7-24 AND HE WAS IN ATTENDANCE. HE WILL NOT BE ON TODAY'S CALL SINCE YOU INADVERTANTLY FIRED HIM YESTERDAY.

Given these compliance issues, retaining Ryan to work in these areas conflicts with the PCI DSS 4 standards. His non-compliance and refusal to adhere to required protocols undermine our efforts to maintain these critical standards.

Please provide specific details regarding the necessity of retaining Ryan's services and ensure that it does not conflict with our PCI DSS 4 compliance requirements. I would like you to know that understanding your rationale and how it aligns with these standards is essential for moving forward.

Thank you for your attention to this matter. I look forward to your response to resolve this issue in compliance with our obligations.

Exhibit 19H



6.2.1 ✓

Bespoke and custom software are developed securely, as follows:

- Based on industry standards and/or best practices for secure development.
- Bullet intentionally left blank for this SAQ.
- Bullet intentionally left blank for this SAQ.

6.2.2 ✓

Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows:

- On software security relevant to their job function and development languages.
- Including secure software design and secure coding techniques.
- Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.

6.2.3.1 ✓

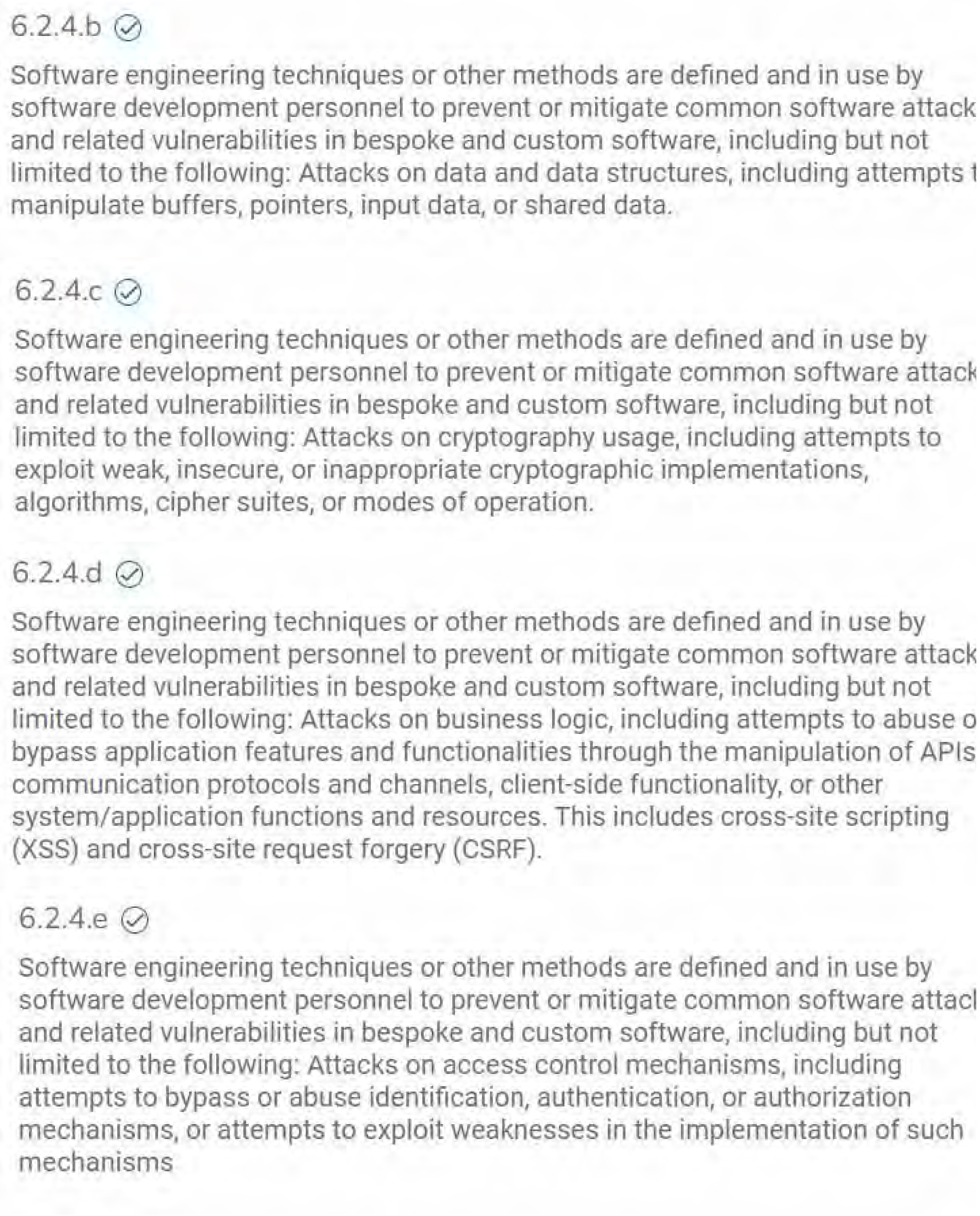
If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are:

- Reviewed by individuals other than the originating code author, and who ar knowledgeable about code-review techniques and secure coding practices.
- Reviewed and approved by management prior to release.

6.2.4.a ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws

Exhibit 19H



6.2.4.b ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on data and data structures, including attempts t manipulate buffers, pointers, input data, or shared data.

6.2.4.c ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation.

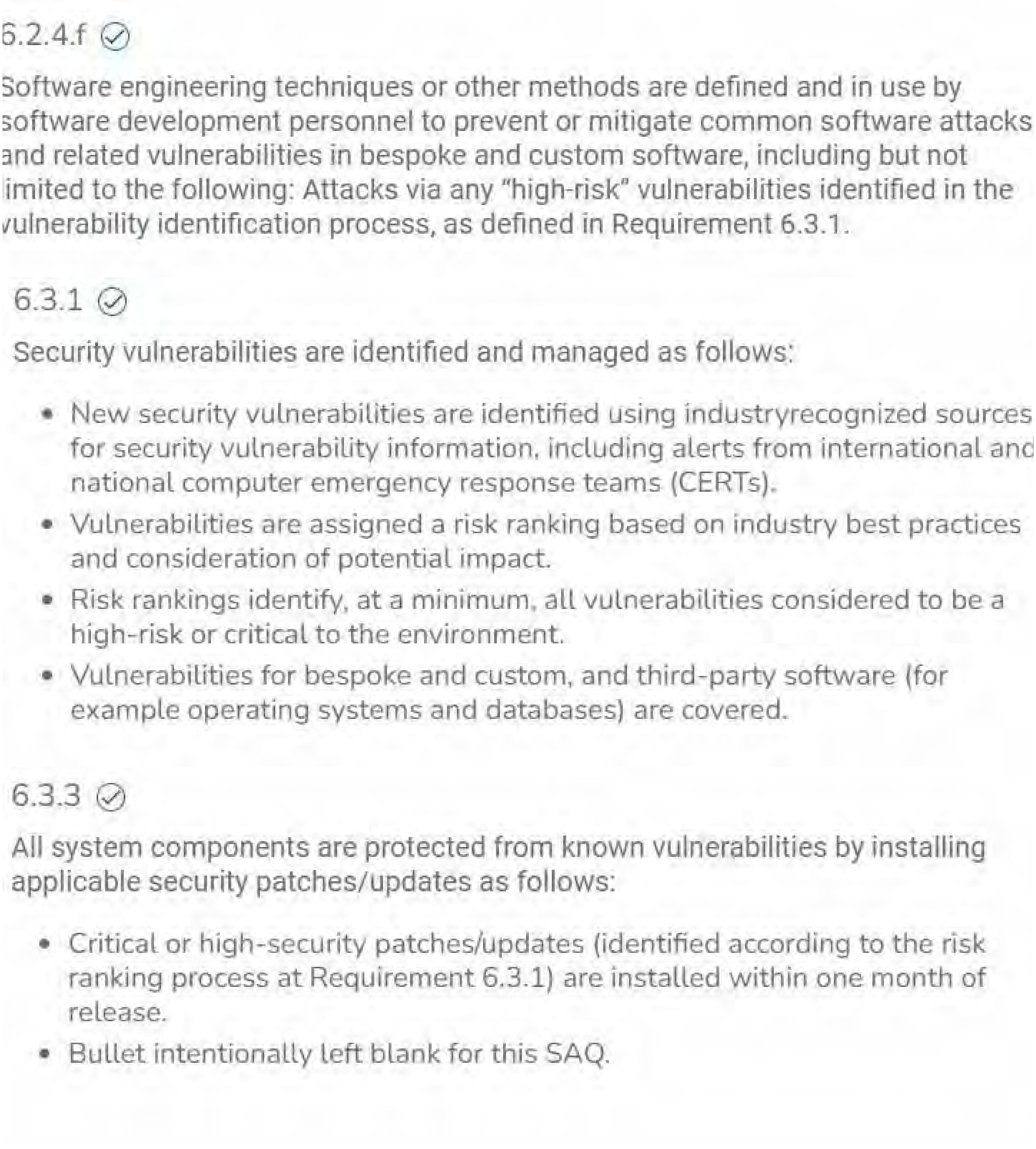
6.2.4.d ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on business logic, including attempts to abuse o bypass application features and functionalities through the manipulation of APIs communication protocols and channels, client-side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF).

6.2.4.e ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacl and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms

Exhibit 19H



6.2.4.f ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks via any "high-risk" vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1.

6.3.1 ✓

Security vulnerabilities are identified and managed as follows:

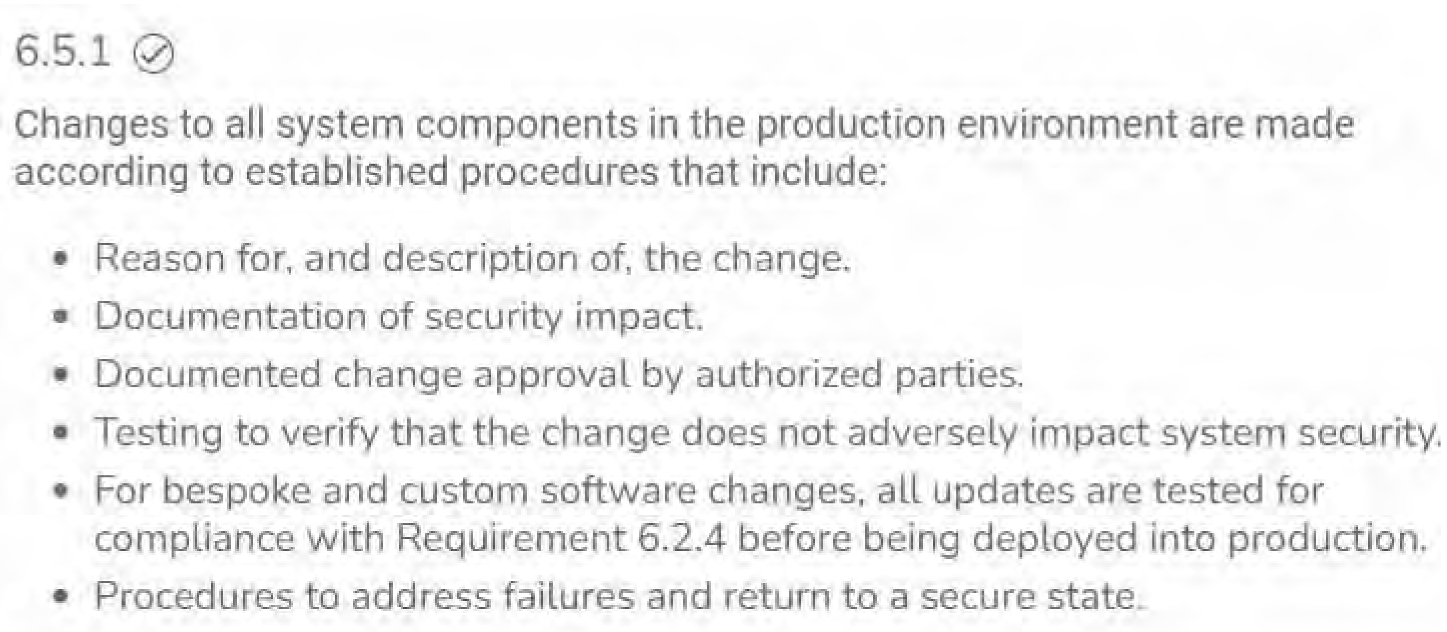
- New security vulnerabilities are identified using industryrecognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).
- Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.
- Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.
- Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.

6.3.3 ✓

All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows:

- Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release.
- Bullet intentionally left blank for this SAQ.

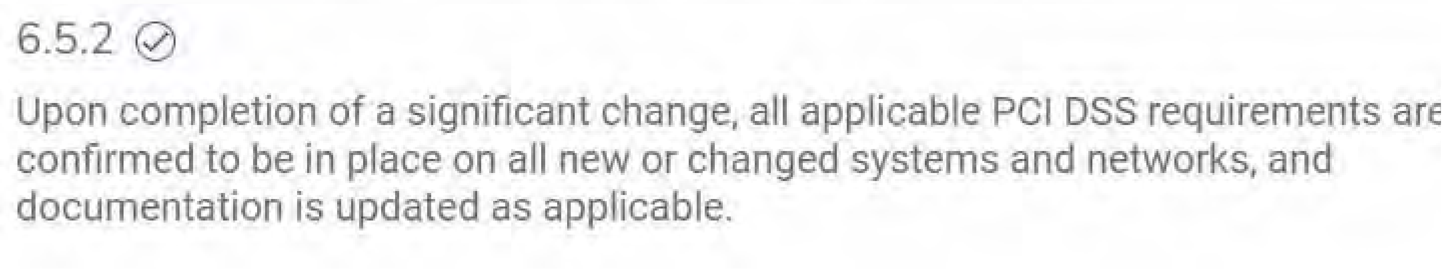
Exhibit 19H



6.5.1 ✓

Changes to all system components in the production environment are made according to established procedures that include:

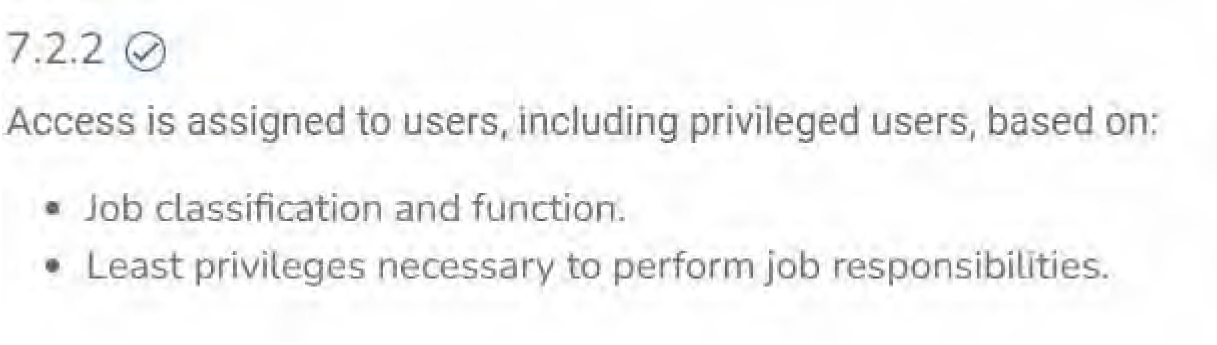
- Reason for, and description of, the change.
- Documentation of security impact.
- Documented change approval by authorized parties.
- Testing to verify that the change does not adversely impact system security.
- For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production.
- Procedures to address failures and return to a secure state.



6.5.2 ✓

Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.

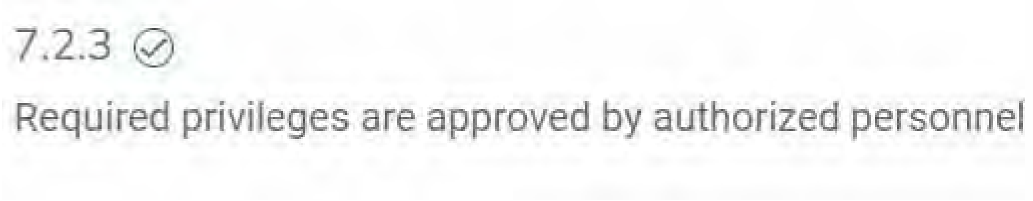
Please provide specific details regarding the necessity of retaining Ryan's services which does not conflict with our PCI DSS 4 compliance requirements. I would like you to know that understanding your rationale and how it aligns with these standards is essential for moving forward by assigning him permissions that will give him the least privileges necessary while not performing tasks listed above or otherwise in the PCI DSS 4.



7.2.2 ✓

Access is assigned to users, including privileged users, based on:

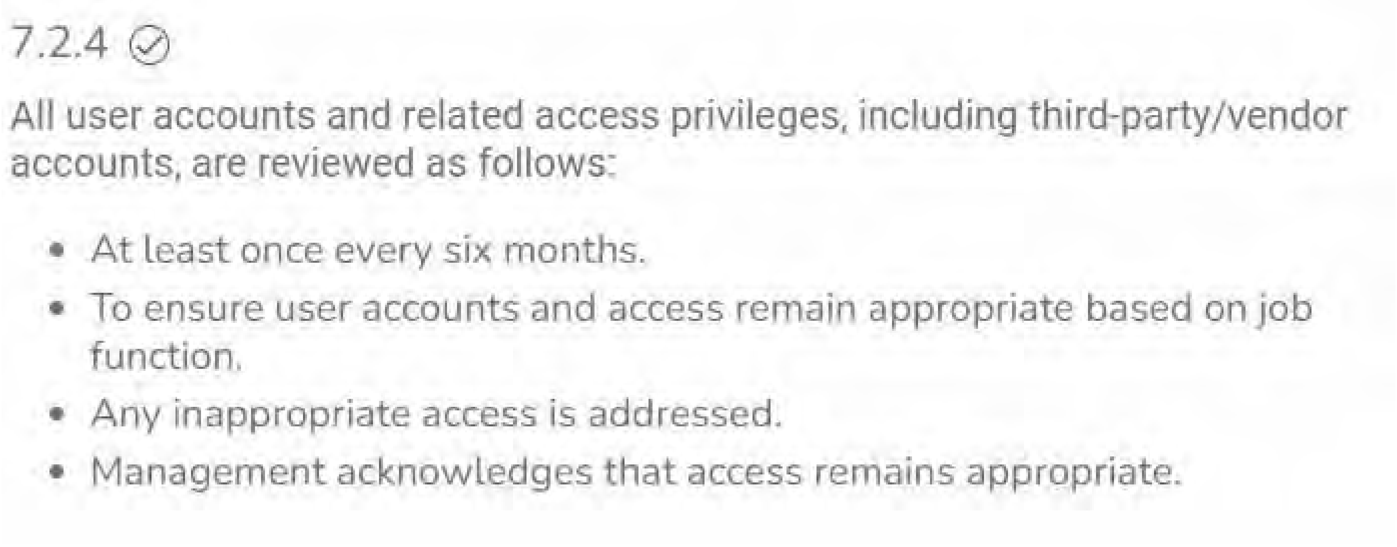
- Job classification and function.
- Least privileges necessary to perform job responsibilities.



7.2.3 ✓

Required privileges are approved by authorized personnel

Exhibit 19H



7.2.4 ✓

All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows:

- At least once every six months.
- To ensure user accounts and access remain appropriate based on job function.
- Any inappropriate access is addressed.
- Management acknowledges that access remains appropriate.

Thank you for your attention to this matter. I look forward to your response and to resolving this issue in accordance with our obligations.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

Exhibit 19I

From:	**Ryan Wagner**
Sent:	**Tuesday, May 21, 2024 5:14 PM**
To:	**Matt Norris; Glenn Norris**
Cc:	**Justin Drummond; Rich Hartman; Karen Debus**
Subject:	**Re: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS**

To be clear, I don't have an issue with us testing a 2nd AVD. I have issues with both staying live and doubling the cost. if we needed both sets of resources, then they should be in the same environment and load balanced; alternatively, if we didn't need them both, then why pay for both?

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093

www.planetfitness.com

"Culture eats strategy for breakfast"

From: Matt Norris <Matt.Norris@ohanagp.com>
Sent: Tuesday, May 21, 2024 5:07 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>; Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>
Subject: RE: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

Hi Ryan,

I disagree with your performance concerns section below, Ryan Brooks setting up the 2nd AVD environment has helped performance improve significantly since the initial implementation that you oversaw in September.

Matt Norris
VP of Finance
Ohana Growth Partners, LLC

Exhibit 19I

OHANA
Growth Partners

office 410-252-8058 x121
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 4:56 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: Re: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

Thank you for your email. I understand your concerns and would like to clarify the situation regarding Ryan Brooks' access and our compliance requirements.

Compliance and Access Issues:

Yesterday, I consulted with PFHQ about how to handle situations where personnel had not completed required training. Before I could act on the conversation, Ryan Brooks informed me he didn't have time for a mandatory 15-minute meeting, and he had already stated he couldn't complete the required training or other tasks assigned to him. Consequently, I removed him to resolve the block to completing the SAQ, as instructed by PFHQ.

Overnight Changes:

The compliance issues did not change overnight. What changed was the final decision to remove Ryan after he explicitly refused to engage in critical compliance activities. Reinstating his access today would violate PCI DSS 4.0 standards, as I have already informed the head of corporate security that the compliance issue was resolved by terminating his access.

Performance Concerns:

The issues identified by Matt, as well as numerous concerns raised by the accounting department, reflect the quality of Ryan's work. While being responsive is important, it is more critical to ensure that work aligns with our strategic objectives and compliance requirements and does not result in these problems existing. Since September/October, Ryan's recommendations have moved us further from resolution, as evidenced by the ongoing issues highlighted in Matt's email.

Ryan's inability to complete tasks assigned to him and his mismanagement of resources (e.g., setting up a second AVD environment, doubling costs, ignoring Microsoft's recommendations) demonstrate a lack of alignment with our strategic direction. His actions, including making unauthorized changes, have exacerbated our challenges rather than resolving them.

Historical Context:

From the start of the emergency migration project, Ryan proposed outdated solutions, like reinvesting in an old AC system instead of modernizing our platform. Following my HR complaint in November, you stopped supporting the initial proposal and allowed Ryan to make changes against our needs, often in secret. Before my FMLA leave, you

Exhibit 19I

reinstated his access despite my concerns. Since FMLA, you and Ryan have been in charge of the IT department. Recently, you informed me I should no longer step back, allowing me to re-establish control and initiate daily standups and other processes to get the team back on track.

Next Steps:

Given the situation:

Ryan must complete the PCI DSS compliance training and participate in the required processes before his access can be reinstated.
Restoring his access without meeting these requirements would jeopardize our PCI DSS 4.0 compliance.
I am committed to resolving these issues in a manner that upholds our compliance standards and addresses our operational needs. Please review the data, recommendations, and conclusions from Microsoft and our current state of issues, which collectively indicate that Ryan is not currently qualified to manage our cloud environment.

We can review these concerns with the head of corporate security, and if I understand why it must happen today, perhaps I can offer a solution that does not result in PCI compliance issues.

Thank you for your understanding and cooperation.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 4:28 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: RE: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

How was Ryan Brooks allowed access yesterday and not today? What changed overnight, it does not make sense that compliance issues were just discovered and changed overnight.

I do not think your stance flies.

Please do as I have instructed you. He will take the test.

Exhibit 19I

See Matt's reason why we need him. Look at attached email.

Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 3:38 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: Re: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

@Glenn Norris

Thank you for your email. I understand your urgency regarding Ryan Brooks' access and want to ensure we handle this appropriately while maintaining our compliance with PCI DSS 4.0 standards.

1. **Mandates and Requirements:**

    - PFHQ mandates compliance with PCI DSS 4.0, which outlines the specific requirements for all personnel with access to sensitive data and systems. This includes mandatory training and participation in key security processes.

2. **Attestation Filings:**

    - PFHQ instructed me to complete the attestation filings, which are necessary to certify our compliance with PCI DSS 4.0. These filings were submitted to our compliance auditors and relevant regulatory bodies to confirm that we meet all required security standards.

3. **Ryan Brooks' Access:**

    - Restoring Ryan Brooks' access without him completing the required training and participating in mandated security processes would violate our PCI DSS 4.0 compliance. This could jeopardize our certification and the security of our systems.

Could you please clarify the consequences you foresee if we do not restore Ryan's access today? Understanding your concerns will help us address them while ensuring we remain compliant with PCI DSS 4.0 standards.

Exhibit 19I

I must emphasize that compliance with these standards is critical to our operations and security. I am committed to resolving this situation as quickly as possible within the bounds of our compliance requirements.

Please let me know how you would like to proceed, and we can work together to find a solution that maintains our compliance and addresses your needs.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

“Culture eats strategy for breakfast”

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 3:26 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: RE: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

1. Please explain who is mandating this and what it entails.
2. Stop filing attestation filings- who gets these and why were they sent in the last 24 hours?
3. I WANT RYAN’S ACCESS RESTORED TODAY. CONFIRM WHEN THIS IS COMPLETED

Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

“Culture eats strategy for breakfast”

Exhibit 19I

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 2:08 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: Re: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

@Glenn Norris I hope this message finds you well. I appreciate your prompt response regarding Ryan Brooks' compliance and performance. I would like to address the points you raised to ensure clarity and alignment with our compliance requirements and performance expectations.

Compliance Allegations:
Regarding the compliance allegations, it is crucial to clarify that all team members, including vendors, must complete the required PCI DSS compliance training. This is a non-negotiable requirement to maintain our certification and ensure our systems' security and integrity. If Ryan was previously informed that he did not need to complete this training, that was incorrect, and I appreciate his willingness to rectify this.

Compliance Training Requirement:
Ryan must complete the PCI DSS compliance training before he can resume any work, as our attestation has already been filed.
Additional Compliance Requirements:

Beyond the training, Ryan's access has been restricted due to his lack of participation in several PCI DSS-required processes. These include:

Participation in daily standup meetings
Involvement in the change control review board
Engagement in the pipeline for code publishing
Adherence to other necessary procedures
Ryan has previously refused to engage in these processes, which are critical for maintaining our compliance. Additionally, the partial work he has completed has not met PCI DSS compliance standards, and I have had to redo this work to align with our requirements.

Access and Admin Rights:
Regarding your directive to restore Ryan's admin rights immediately, I must emphasize that any such action must comply with our PCI DSS 4 standards. Until Ryan completes the required compliance steps and demonstrates his understanding of PCI DSS requirements, he will not be able to make changes to any system as an administrator. This includes both his software engineer responsibilities and sufficient training for administration.

Next Steps:

Ryan must complete the PCI DSS compliance training immediately.HE IS DOING THIS
Ryan must participate in all PCI DSS required processes, including daily standups, change control review boards, and code publishing pipelines. I DO NOT AGREE
After Ryan completes the training and engages in these processes, we need detailed information on the specific tasks you want him to perform. This will allow us to assign him the least privileged access necessary to maintain PCI compliance.

Exhibit 19I

If you feel it would be helpful, I am open to arranging a meeting with the corporate head of security to weigh in on these items and provide additional perspective on maintaining our compliance and security standards. NO THANK YOU

Thank you for your understanding and cooperation in ensuring we maintain our compliance and security standards. I look forward to resolving this matter collaboratively. I DO NOT AGREE WITH YOUR POSITIONS

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 1:48 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>; Glenn Norris <glenn@ohanagp.com>
Subject: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

Ryan, I do not agree with your performance and compliance allegations of Ryan Brooks. I asked him if he was required by you to complete the compliance PCI tests and he was adamant that you stated months ago that he did not need to complete this. He is willing to do it. This is straight from Ryan Brooks.

Regarding his performance, we need to have a conversation on your expectations and role for BC/RB. In my opinion, he has been and still is a valued vendor for our IT needs .

Please ask Justin, Rich, Matt or Karen(and others) how they do or do not value his contribution to our IT needs.

As I stated in our call earlier today, I want his admin rights restored today. There was no discussion with me about this action – I do not approve.

SEE COMMENTS IN RED BELOW

Exhibit 19I

Thank you, Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 1:16 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>
Subject: Ryan Brooks - More Info Needed

@Glenn Norris, I hope you're doing well. I am seeking clarification regarding your directive to retain Ryan Brooks in the IT Department. When we talked today, you expressed a specific need for his services, despite my concerns about his performance and our compliance requirements.

In addition, As part of our compliance with PCI DSS 4 standards, which I recently certified after significant efforts, every team member must meet the requirements. Ryan Brooks' refusal to follow proper procedures and complete the required upskill training posed a substantial obstacle to maintaining PCI DSS 4 unless he is able to do the things that I have required of him.

To clarify:

1. **Security Training**: Ryan has not completed the mandatory security training, which disqualifies him from being employed as a software engineer under PCI DSS 4 standards. HE WILL DO THIS IF IT IS REQUIRED.

2. **Code Review Process**: He has been unable to participate in the code review process, making him unsuitable for automation or SQL work. WHAT IS THE REQUIRED TIME INVESTMENT HERE?

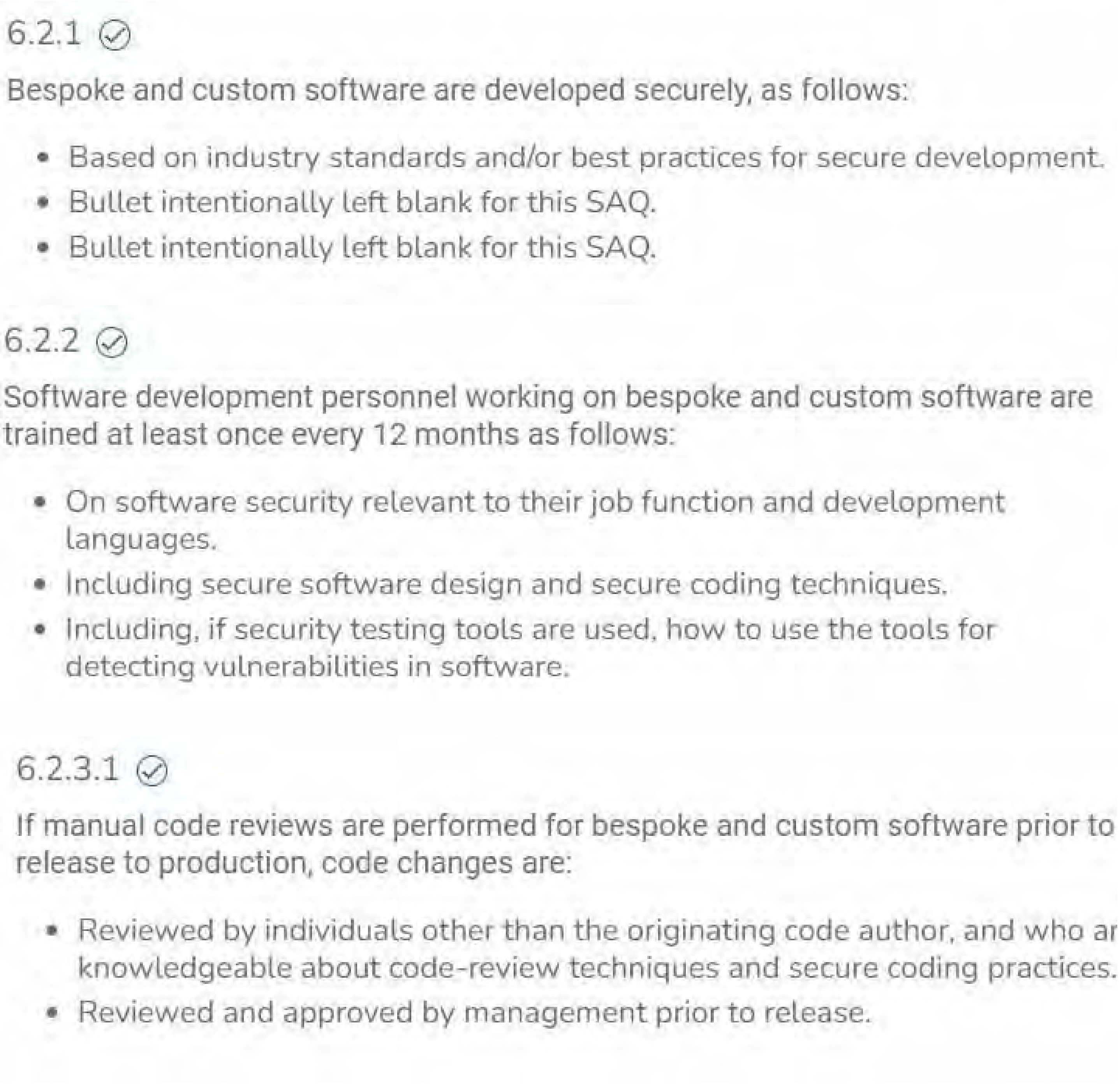
3. **Change Control Review Board**: Ryan's lack of participation in the change control review board precludes him from performing any sysadmin tasks or handling M365 or Azure responsibilities. HE HAS BEEN ON EVERY TUESDAY 230 CALL AND YOU GHOSTED THAT CALL ON 5-7-24 AND HE WAS IN ATTENDANCE. HE WILL NOT BE ON TODAY'S CALL SINCE YOU INADVERTANTLY FIRED HIM YESTERDAY.

Given these compliance issues, retaining Ryan to work in these areas conflicts with the PCI DSS 4 standards. His non-compliance and refusal to adhere to required protocols undermine our efforts to maintain these critical standards.

Please provide specific details regarding the necessity of retaining Ryan's services and ensure that it does not conflict with our PCI DSS 4 compliance requirements. I would like you to know that understanding your rationale and how it aligns with these standards is essential for moving forward.

Exhibit 19I

Thank you for your attention to this matter. I look forward to your response to resolve this issue in compliance with our obligations.



6.2.1 ✓

Bespoke and custom software are developed securely, as follows:

- Based on industry standards and/or best practices for secure development.
- Bullet intentionally left blank for this SAQ.
- Bullet intentionally left blank for this SAQ.

6.2.2 ✓

Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows:

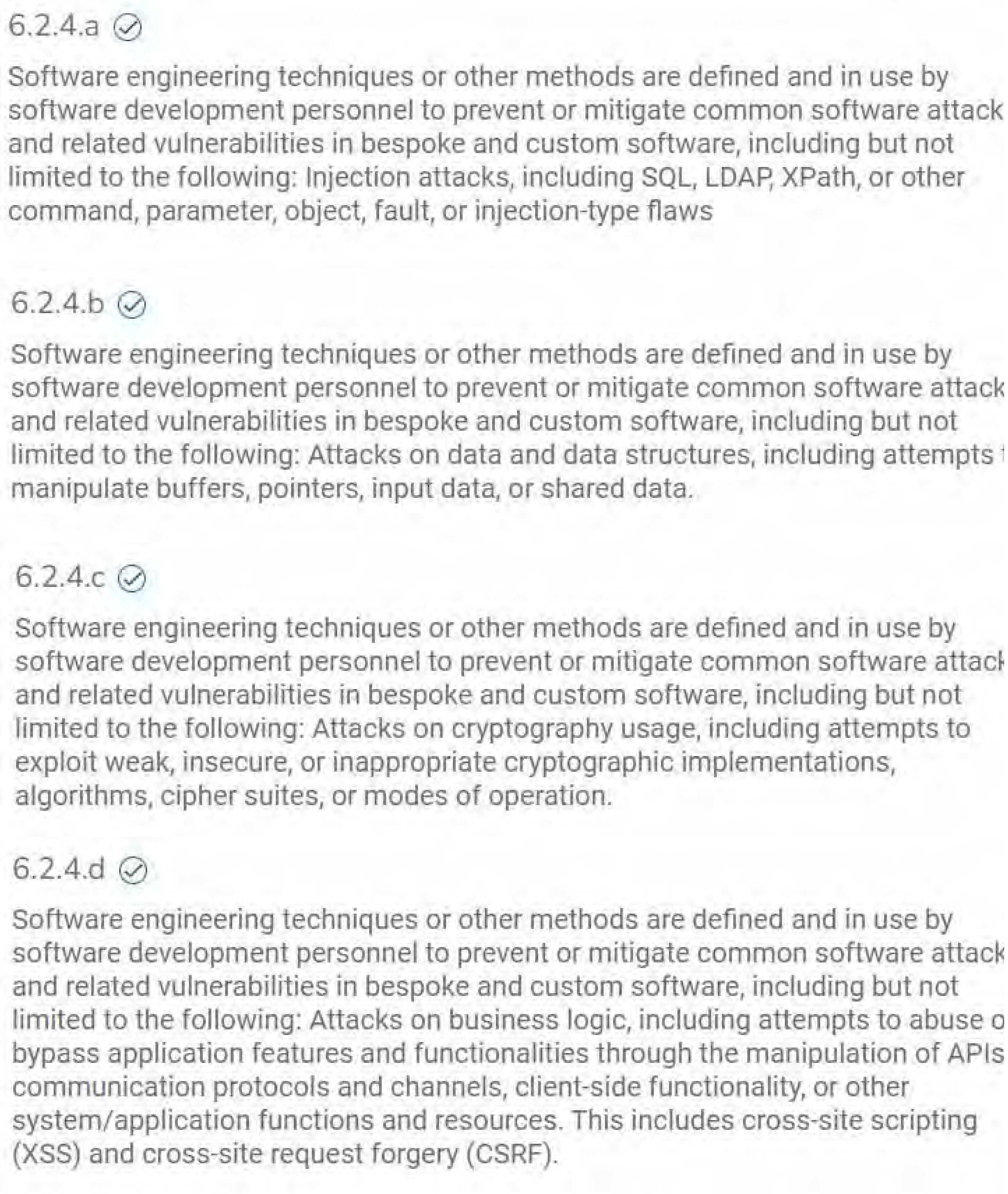
- On software security relevant to their job function and development languages.
- Including secure software design and secure coding techniques.
- Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.

6.2.3.1 ✓

If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are:

- Reviewed by individuals other than the originating code author, and who ar knowledgeable about code-review techniques and secure coding practices.
- Reviewed and approved by management prior to release.

Exhibit 19I



6.2.4.a ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws

6.2.4.b ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on data and data structures, including attempts manipulate buffers, pointers, input data, or shared data.

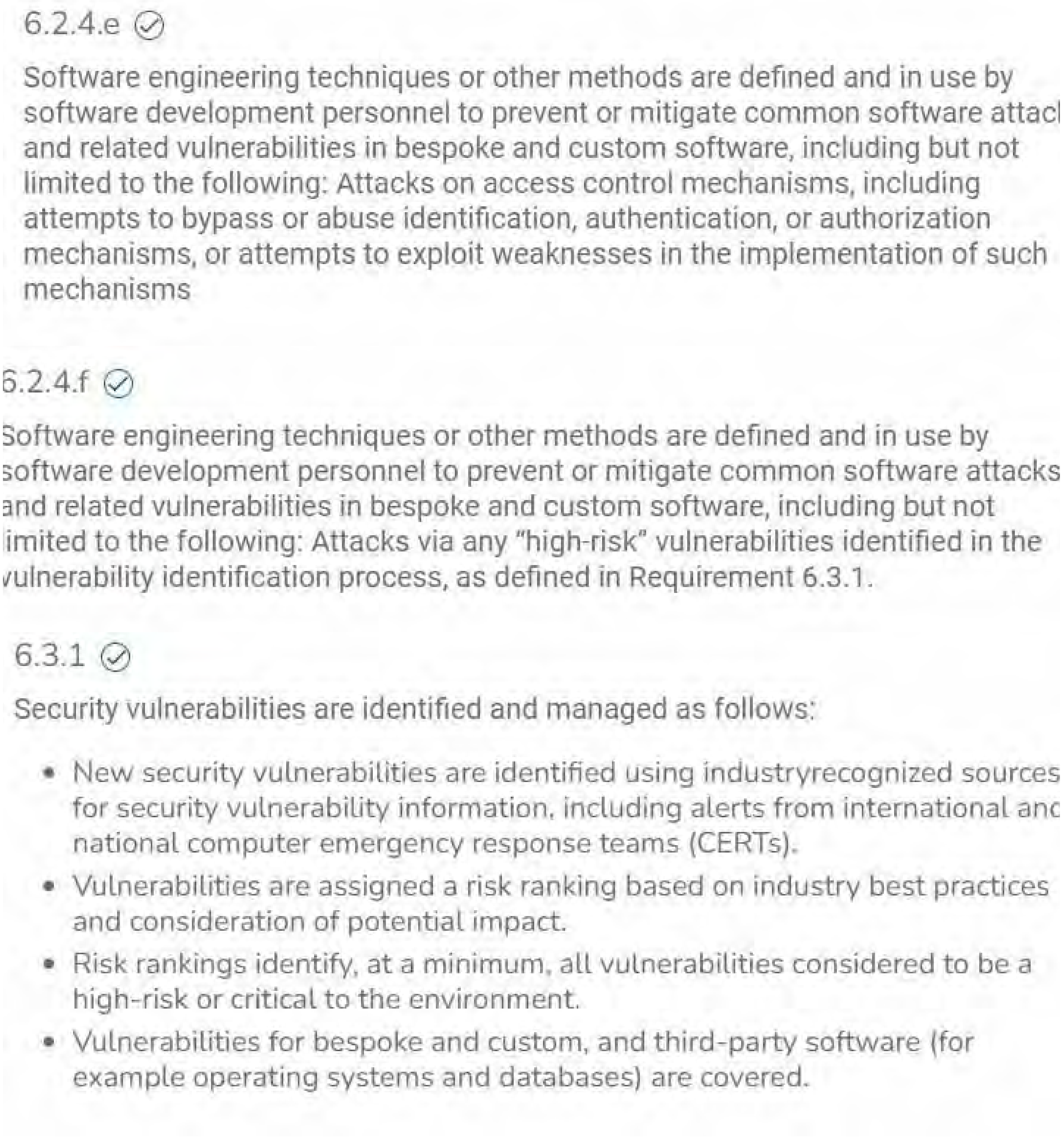
6.2.4.c ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation.

6.2.4.d ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on business logic, including attempts to abuse o bypass application features and functionalities through the manipulation of APIs communication protocols and channels, client-side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF).

Exhibit 19I



6.2.4.e ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacl and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms

6.2.4.f ✓

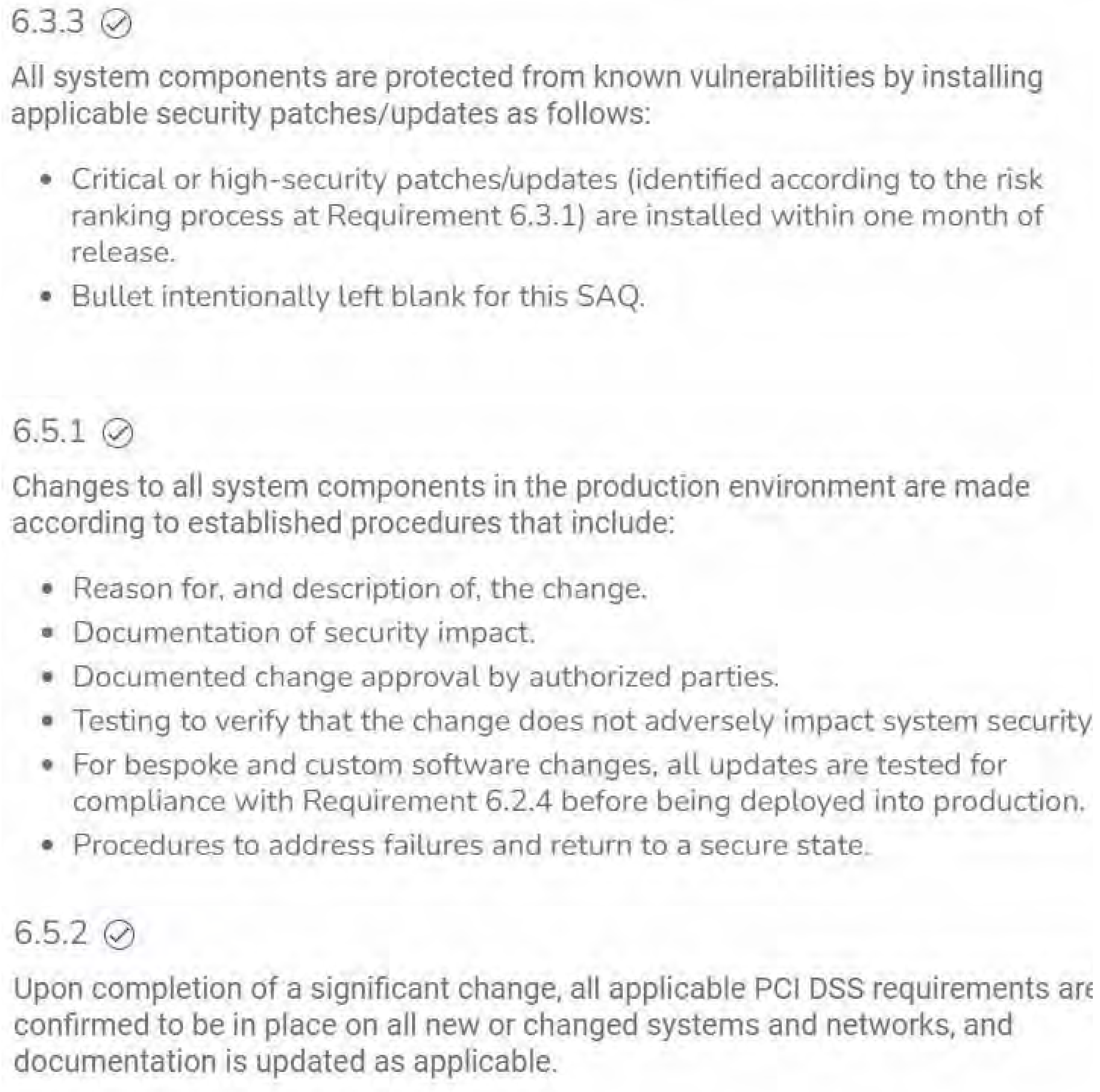
Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not imited to the following: Attacks via any "high-risk" vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1.

6.3.1 ✓

Security vulnerabilities are identified and managed as follows:

- New security vulnerabilities are identified using industryrecognized sources for security vulnerability information, including alerts from international anc national computer emergency response teams (CERTs).
- Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.
- Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.
- Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.

Exhibit 19I



6.3.3 ✓

All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows:

- Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release.
- Bullet intentionally left blank for this SAQ.

6.5.1 ✓

Changes to all system components in the production environment are made according to established procedures that include:

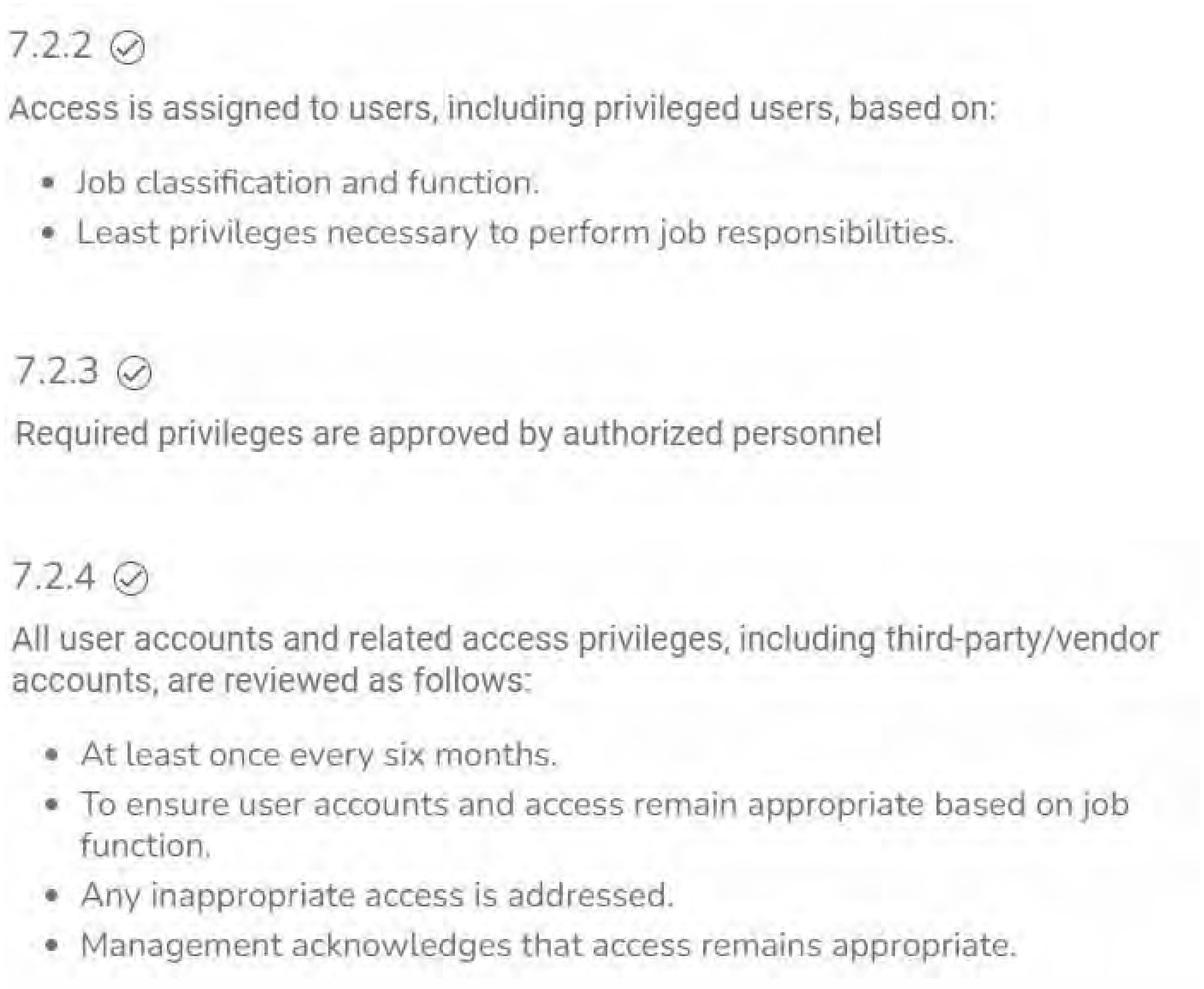
- Reason for, and description of, the change.
- Documentation of security impact.
- Documented change approval by authorized parties.
- Testing to verify that the change does not adversely impact system security
- For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production.
- Procedures to address failures and return to a secure state.

6.5.2 ✓

Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.

Please provide specific details regarding the necessity of retaining Ryan's services which does not conflict with our PCI DSS 4 compliance requirements. I would like you to know that understanding your rationale and how it aligns with these standards is essential for moving forward by assigning him permissions that will give him the least privileges necessary while not performing tasks listed above or otherwise in the PCI DSS 4.

Exhibit 19I



7.2.2 ✓

Access is assigned to users, including privileged users, based on:

- Job classification and function.
- Least privileges necessary to perform job responsibilities.

7.2.3 ✓

Required privileges are approved by authorized personnel

7.2.4 ✓

All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows:

- At least once every six months.
- To ensure user accounts and access remain appropriate based on job function.
- Any inappropriate access is addressed.
- Management acknowledges that access remains appropriate.

Thank you for your attention to this matter. I look forward to your response and to resolving this issue in accordance with our obligations.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

Exhibit 19I

OHANA
Growth Partners

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

Exhibit 19J

Ryan Dillon-Capps

From:	**Ryan Wagner**
Sent:	**Tuesday, May 21, 2024 5:22 PM**
To:	**C. Victor Brick**
Subject:	**Fw: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS**

I wish we could have better reasons to communicate. You should know what I am being ordered to do under duress.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093

www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 5:12 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: Re: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

I acknowledge your directive and understand the urgency of the situation. However, I must reiterate the compliance risks associated with reinstating Ryan Brooks' access without him completing the necessary PCI DSS 4.0 training and processes.

As the head of IT, my primary responsibility is to ensure that we maintain compliance with all regulatory standards. Restoring Ryan's access without meeting these requirements places our PCI DSS 4.0 certification and the company at significant risk. While I am prepared to follow your instructions, I must stress that this action is being undertaken under duress due to your explicit directive.

I have reached out to Geoff VanMaastricht, our head of corporate security, to seek his assistance in finding a solution that balances our compliance obligations with your request. Here is the email I sent to him, which includes you and President Justin Drummond in the loop:

Ryan Wagner

Exhibit 19J

Vice President of IT
Ohana Growth Partners, LLC

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner Ryan.Wagner@ohanagp.com
Sent: Tuesday, May 21, 2024 5:09 PM
To: Geoff VanMaastricht Geoff.VanMaastricht@pfhq.com
Cc: Glenn Norris glenn@ohanagp.com; Justin Drummond Justin.Drummond@ohanagp.com
Subject: SAQ - PCI Compliance: We need your assistance

@Geoff VanMaastricht, Would you be available for a meeting tomorrow to discuss this and related PCI Compliance concerns? I am being told to reinstate the same person, but they refuse to do the training, take part in the code review, change control, or any other process to maintain compliance. I don't know what to do and could use your assistance to find a solution that works for our CFO as well as meet the compliance requirements.

To mitigate these risks and protect our compliance standing, I propose the following steps:

Immediate Compliance Training: Expedite Ryan's PCI DSS 4.0 compliance training and ensure it is completed as a top priority.
Temporary Limited Access: Provide Ryan with limited access necessary for immediate tasks, under close monitoring, until he completes the required training and processes.
Documented Agreement: Document this course of action, including the acknowledgment that this decision is made under duress, to protect both the company and ourselves, ensuring we have a record of our compliance efforts and the rationale behind these decisions.
I am available to discuss this further and facilitate any immediate actions required to address your concerns while maintaining our compliance obligations.

Please let me know how you would like to proceed.

Best regards,

This message may include text created with the help of natural language processing.

Book time to meet with me

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 5:05 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: RE: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

Rich, please prepare a write up for me .

Exhibit 19J

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 5:02 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: Re: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

@Glenn Norris

Thank you for your prompt response. I understand the urgency of your request, but I must reiterate the compliance requirements and potential risks involved in reinstating Ryan Brooks' access without completing the necessary PCI DSS 4.0 training and processes.

Reinstating his access without compliance would put our certification at risk and could have serious legal and security implications for the company. As the head of IT, I have a responsibility to ensure that we adhere to these standards.

Given the gravity of the situation and your directive, I propose a meeting tomorrow morning with you, myself, and the head of corporate security to discuss how we can address this matter without compromising our compliance obligations. This will allow us to find a solution that meets your needs while safeguarding our compliance and security standards.

Please confirm a suitable time for this meeting.

Thank you for your understanding.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

Exhibit 19J

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 4:59 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: RE: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

If Ryan Brooks does not have access by tomorrow morning , you will be written up for insubordination. Is that clear? Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 4:56 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: Re: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

Thank you for your email. I understand your concerns and would like to clarify the situation regarding Ryan Brooks' access and our compliance requirements.

Compliance and Access Issues:

Yesterday, I consulted with PFHQ about how to handle situations where personnel had not completed required training. Before I could act on the conversation, Ryan Brooks informed me he didn't have time for a mandatory 15-minute meeting, and he had already stated he couldn't complete the required training or other tasks assigned to him. Consequently, I removed him to resolve the block to completing the SAQ, as instructed by PFHQ.

Overnight Changes:

Exhibit 19J

The compliance issues did not change overnight. What changed was the final decision to remove Ryan after he explicitly refused to engage in critical compliance activities. Reinstating his access today would violate PCI DSS 4.0 standards, as I have already informed the head of corporate security that the compliance issue was resolved by terminating his access.

Performance Concerns:

The issues identified by Matt, as well as numerous concerns raised by the accounting department, reflect the quality of Ryan's work. While being responsive is important, it is more critical to ensure that work aligns with our strategic objectives and compliance requirements and does not result in these problems existing. Since September/October, Ryan's recommendations have moved us further from resolution, as evidenced by the ongoing issues highlighted in Matt's email.

Ryan's inability to complete tasks assigned to him and his mismanagement of resources (e.g., setting up a second AVD environment, doubling costs, ignoring Microsoft's recommendations) demonstrate a lack of alignment with our strategic direction. His actions, including making unauthorized changes, have exacerbated our challenges rather than resolving them.

Historical Context:

From the start of the emergency migration project, Ryan proposed outdated solutions, like reinvesting in an old AC system instead of modernizing our platform. Following my HR complaint in November, you stopped supporting the initial proposal and allowed Ryan to make changes against our needs, often in secret. Before my FMLA leave, you reinstated his access despite my concerns. Since FMLA, you and Ryan have been in charge of the IT department. Recently, you informed me I should no longer step back, allowing me to re-establish control and initiate daily standups and other processes to get the team back on track.

Next Steps:

Given the situation:

Ryan must complete the PCI DSS compliance training and participate in the required processes before his access can be reinstated.
Restoring his access without meeting these requirements would jeopardize our PCI DSS 4.0 compliance.
I am committed to resolving these issues in a manner that upholds our compliance standards and addresses our operational needs. Please review the data, recommendations, and conclusions from Microsoft and our current state of issues, which collectively indicate that Ryan is not currently qualified to manage our cloud environment.

We can review these concerns with the head of corporate security, and if I understand why it must happen today, perhaps I can offer a solution that does not result in PCI compliance issues.

Thank you for your understanding and cooperation.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

Exhibit 19J

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 4:28 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: RE: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

How was Ryan Brooks allowed access yesterday and not today? What changed overnight, it does not make sense that compliance issues were just discovered and changed overnight.

I do not think your stance flies.

Please do as I have instructed you. He will take the test.

See Matt's reason why we need him. Look at attached email.

Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 3:38 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: Re: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

@Glenn Norris

Thank you for your email. I understand your urgency regarding Ryan Brooks' access and want to ensure we handle this appropriately while maintaining our compliance with PCI DSS 4.0 standards.

Exhibit 19J

1. **Mandates and Requirements:**
   - PFHQ mandates compliance with PCI DSS 4.0, which outlines the specific requirements for all personnel with access to sensitive data and systems. This includes mandatory training and participation in key security processes.
2. **Attestation Filings:**
   - PFHQ instructed me to complete the attestation filings, which are necessary to certify our compliance with PCI DSS 4.0. These filings were submitted to our compliance auditors and relevant regulatory bodies to confirm that we meet all required security standards.
3. **Ryan Brooks' Access:**
   - Restoring Ryan Brooks' access without him completing the required training and participating in mandated security processes would violate our PCI DSS 4.0 compliance. This could jeopardize our certification and the security of our systems.

Could you please clarify the consequences you foresee if we do not restore Ryan's access today? Understanding your concerns will help us address them while ensuring we remain compliant with PCI DSS 4.0 standards.

I must emphasize that compliance with these standards is critical to our operations and security. I am committed to resolving this situation as quickly as possible within the bounds of our compliance requirements.

Please let me know how you would like to proceed, and we can work together to find a solution that maintains our compliance and addresses your needs.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 3:26 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus

Exhibit 19J

<karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: RE: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

1. Please explain who is mandating this and what it entails.
2. Stop filing attestation filings- who gets these and why were they sent in the last 24 hours?
3. I WANT RYAN'S ACCESS RESTORED TODAY. CONFIRM WHEN THIS IS COMPLETED

Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 2:08 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: Re: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

@Glenn Norris I hope this message finds you well. I appreciate your prompt response regarding Ryan Brooks' compliance and performance. I would like to address the points you raised to ensure clarity and alignment with our compliance requirements and performance expectations.

Compliance Allegations:
Regarding the compliance allegations, it is crucial to clarify that all team members, including vendors, must complete the required PCI DSS compliance training. This is a non-negotiable requirement to maintain our certification and ensure our systems' security and integrity. If Ryan was previously informed that he did not need to complete this training, that was incorrect, and I appreciate his willingness to rectify this.

Compliance Training Requirement:
Ryan must complete the PCI DSS compliance training before he can resume any work, as our attestation has already been filed.
Additional Compliance Requirements:

Beyond the training, Ryan's access has been restricted due to his lack of participation in several PCI DSS-required processes. These include:

Participation in daily standup meetings
Involvement in the change control review board
Engagement in the pipeline for code publishing
Adherence to other necessary procedures

Exhibit 19J

Ryan has previously refused to engage in these processes, which are critical for maintaining our compliance. Additionally, the partial work he has completed has not met PCI DSS compliance standards, and I have had to redo this work to align with our requirements.

Access and Admin Rights:
Regarding your directive to restore Ryan's admin rights immediately, I must emphasize that any such action must comply with our PCI DSS 4 standards. Until Ryan completes the required compliance steps and demonstrates his understanding of PCI DSS requirements, he will not be able to make changes to any system as an administrator. This includes both his software engineer responsibilities and sufficient training for administration.

Next Steps:

Ryan must complete the PCI DSS compliance training immediately.HE IS DOING THIS
Ryan must participate in all PCI DSS required processes, including daily standups, change control review boards, and code publishing pipelines. I DO NOT AGREE
After Ryan completes the training and engages in these processes, we need detailed information on the specific tasks you want him to perform. This will allow us to assign him the least privileged access necessary to maintain PCI compliance.

If you feel it would be helpful, I am open to arranging a meeting with the corporate head of security to weigh in on these items and provide additional perspective on maintaining our compliance and security standards. NO THANK YOU

Thank you for your understanding and cooperation in ensuring we maintain our compliance and security standards. I look forward to resolving this matter collaboratively. I DO NOT AGREE WITH YOUR POSITIONS

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 1:48 PM

Exhibit 19J

To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>; Glenn Norris <glenn@ohanagp.com>
Subject: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

Ryan, I do not agree with your performance and compliance allegations of Ryan Brooks. I asked him if he was required by you to complete the compliance PCI tests and he was adamant that you stated months ago that he did not need to complete this. He is willing to do it. This is straight from Ryan Brooks.

Regarding his performance, we need to have a conversation on your expectations and role for BC/RB. In my opinion, he has been and still is a valued vendor for our IT needs .

Please ask Justin, Rich, Matt or Karen(and others) how they do or do not value his contribution to our IT needs.

As I stated in our call earlier today, I want his admin rights restored today. There was no discussion with me about this action – I do not approve.

SEE COMMENTS IN RED BELOW

Thank you, Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 1:16 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>
Subject: Ryan Brooks - More Info Needed

@Glenn Norris, I hope you're doing well. I am seeking clarification regarding your directive to retain Ryan Brooks in the IT Department. When we talked today, you expressed a specific need for his services, despite my concerns about his performance and our compliance requirements.

In addition, As part of our compliance with PCI DSS 4 standards, which I recently certified after significant efforts, every team member must meet the requirements. Ryan Brooks' refusal to follow proper procedures and complete the required upskill training posed a substantial obstacle to maintaining PCI DSS 4 unless he is able to do the things that I have required of him.

To clarify:

Exhibit 19J

1. **Security Training**: Ryan has not completed the mandatory security training, which disqualifies him from being employed as a software engineer under PCI DSS 4 standards. HE WILL DO THIS IF IT IS REQUIRED.

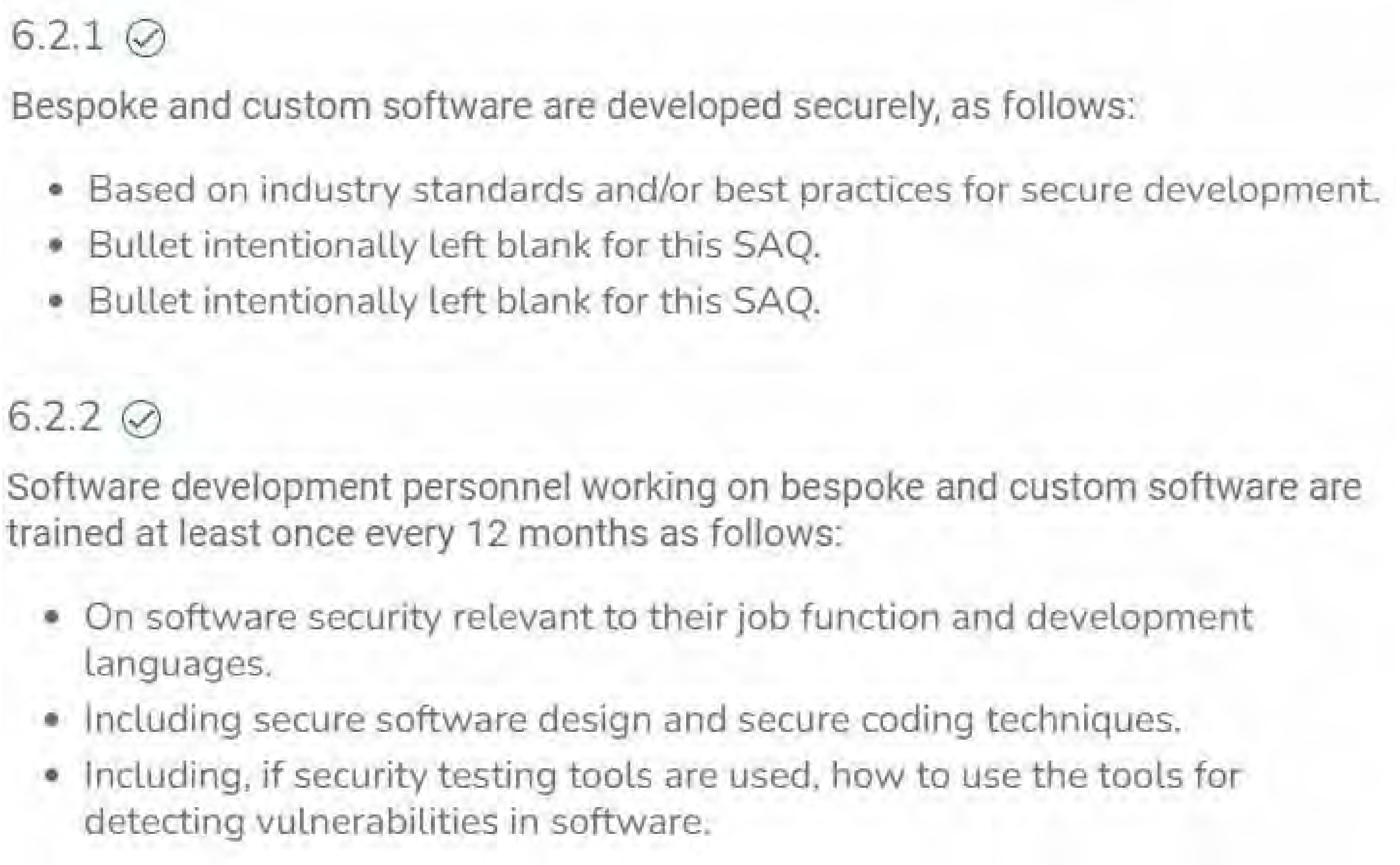
2. **Code Review Process**: He has been unable to participate in the code review process, making him unsuitable for automation or SQL work. WHAT IS THE REQUIRED TIME INVESTMENT HERE?

3. **Change Control Review Board**: Ryan's lack of participation in the change control review board precludes him from performing any sysadmin tasks or handling M365 or Azure responsibilities. HE HAS BEEN ON EVERY TUESDAY 230 CALL AND YOU GHOSTED THAT CALL ON 5-7-24 AND HE WAS IN ATTENDANCE. HE WILL NOT BE ON TODAY'S CALL SINCE YOU INADVERTANTLY FIRED HIM YESTERDAY.

Given these compliance issues, retaining Ryan to work in these areas conflicts with the PCI DSS 4 standards. His non-compliance and refusal to adhere to required protocols undermine our efforts to maintain these critical standards.

Please provide specific details regarding the necessity of retaining Ryan's services and ensure that it does not conflict with our PCI DSS 4 compliance requirements. I would like you to know that understanding your rationale and how it aligns with these standards is essential for moving forward.

Thank you for your attention to this matter. I look forward to your response to resolve this issue in compliance with our obligations.



6.2.1 ✓

Bespoke and custom software are developed securely, as follows:

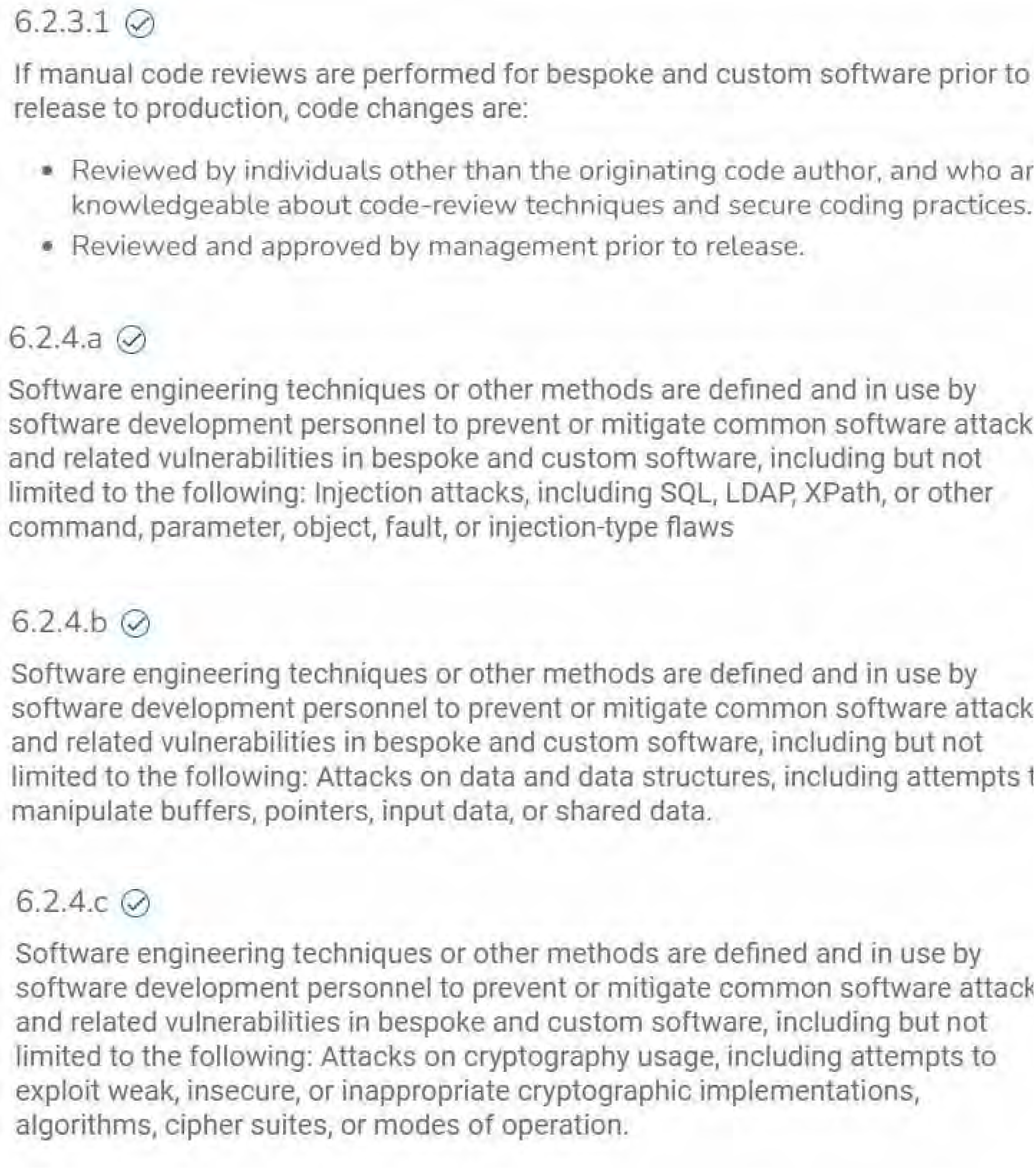
- Based on industry standards and/or best practices for secure development.
- Bullet intentionally left blank for this SAQ.
- Bullet intentionally left blank for this SAQ.

6.2.2 ✓

Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows:

- On software security relevant to their job function and development languages.
- Including secure software design and secure coding techniques.
- Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.

Exhibit 19J



6.2.3.1 ✓

If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are:

- Reviewed by individuals other than the originating code author, and who ar knowledgeable about code-review techniques and secure coding practices.
- Reviewed and approved by management prior to release.

6.2.4.a ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws

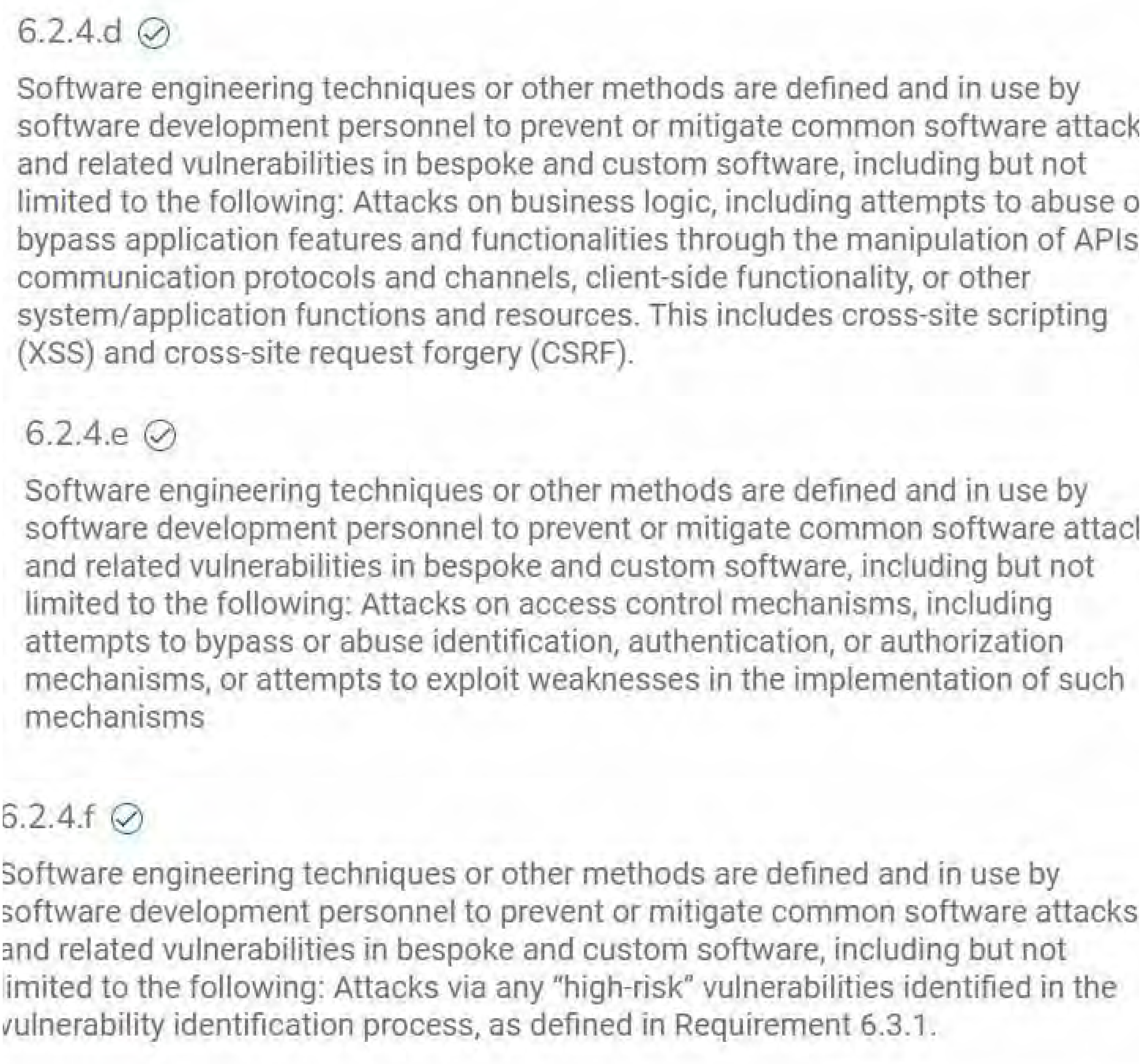
6.2.4.b ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on data and data structures, including attempts t manipulate buffers, pointers, input data, or shared data.

6.2.4.c ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation.

Exhibit 19J



6.2.4.d ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on business logic, including attempts to abuse o bypass application features and functionalities through the manipulation of APIs communication protocols and channels, client-side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF).

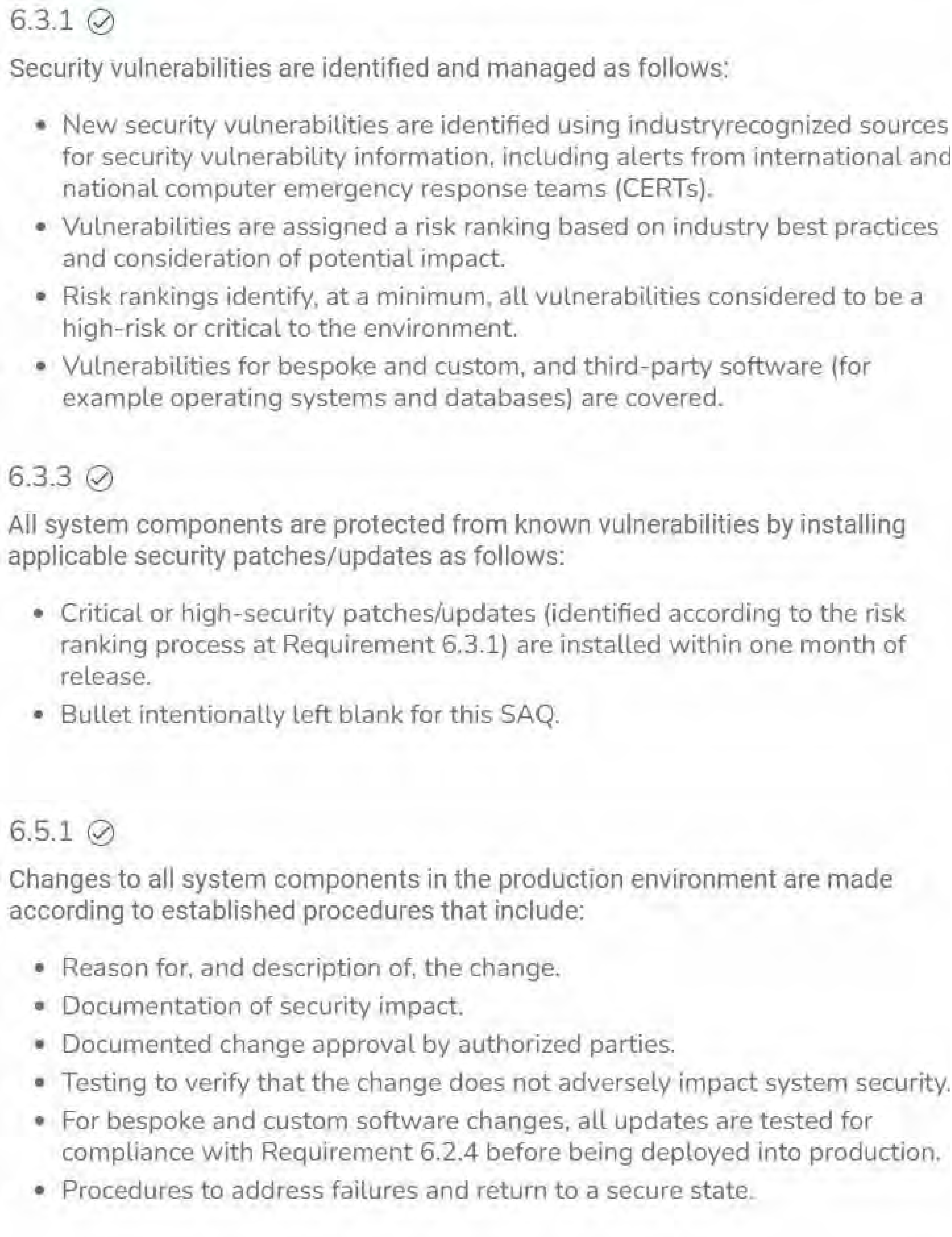
6.2.4.e ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms

6.2.4.f ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks via any “high-risk” vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1.

Exhibit 19J



6.3.1 ✓

Security vulnerabilities are identified and managed as follows:

- New security vulnerabilities are identified using industryrecognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).
- Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.
- Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.
- Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.

6.3.3 ✓

All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows:

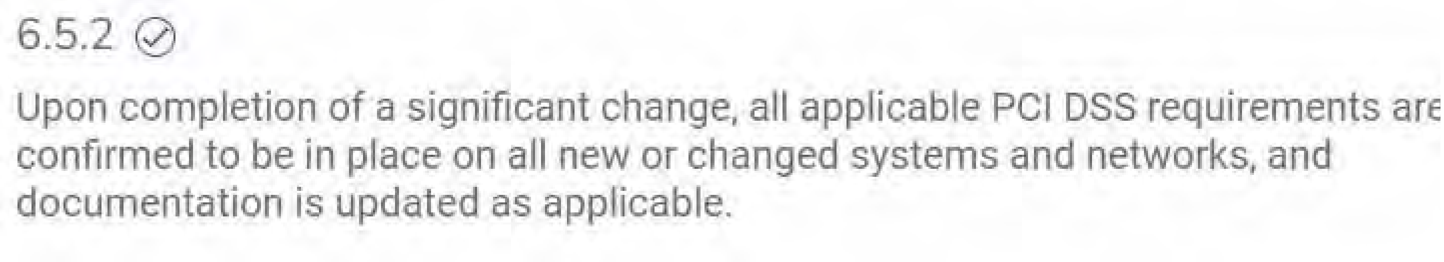
- Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release.
- Bullet intentionally left blank for this SAQ.

6.5.1 ✓

Changes to all system components in the production environment are made according to established procedures that include:

- Reason for, and description of, the change.
- Documentation of security impact.
- Documented change approval by authorized parties.
- Testing to verify that the change does not adversely impact system security.
- For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production.
- Procedures to address failures and return to a secure state.

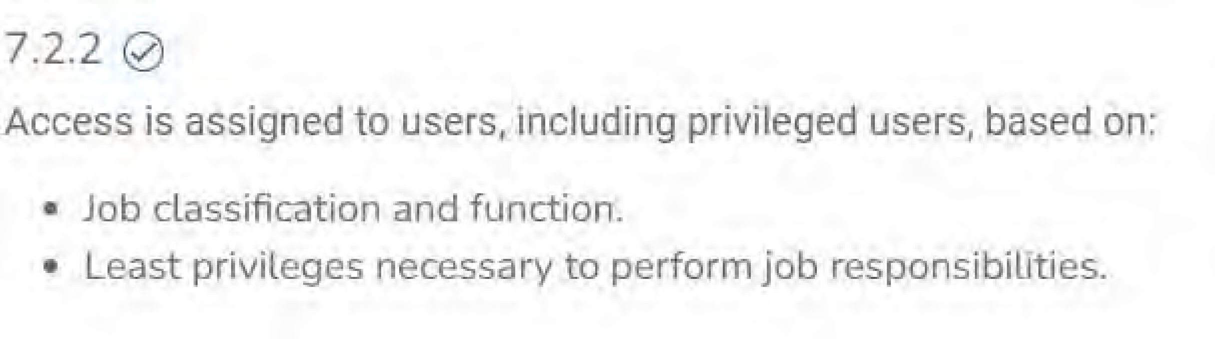
Exhibit 19J



6.5.2 ✓

Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.

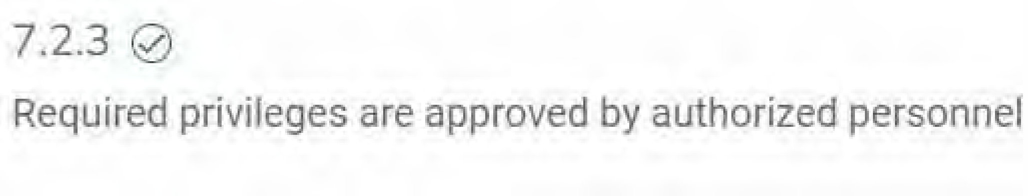
Please provide specific details regarding the necessity of retaining Ryan's services which does not conflict with our PCI DSS 4 compliance requirements. I would like you to know that understanding your rationale and how it aligns with these standards is essential for moving forward by assigning him permissions that will give him the least privileges necessary while not performing tasks listed above or otherwise in the PCI DSS 4.



7.2.2 ✓

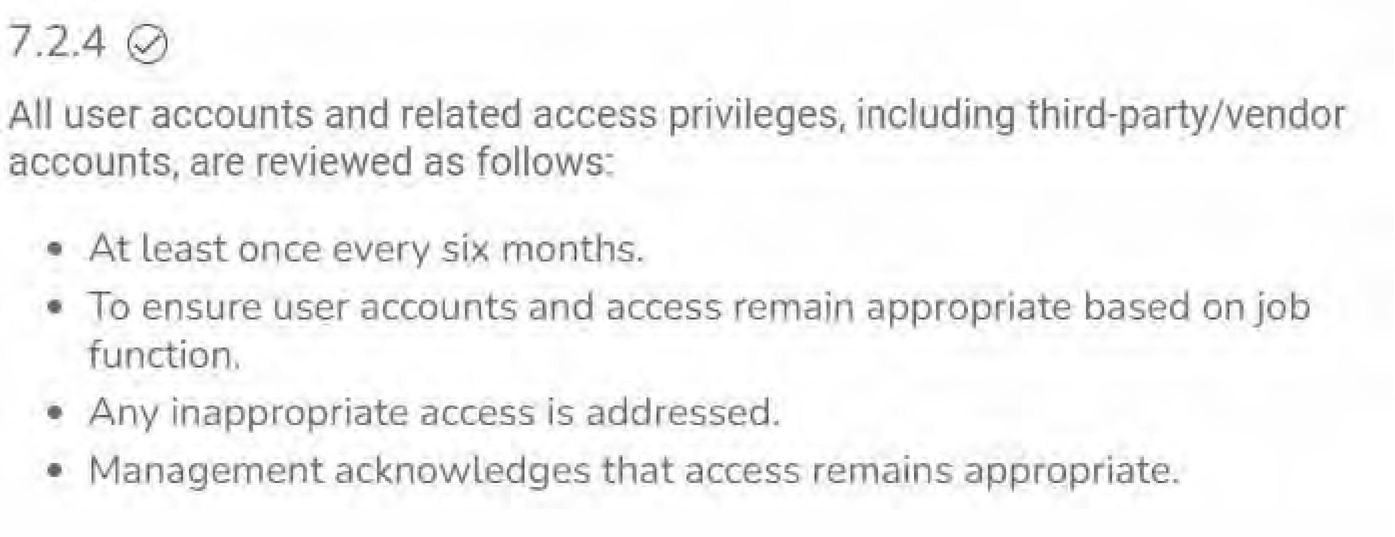
Access is assigned to users, including privileged users, based on:

- Job classification and function.
- Least privileges necessary to perform job responsibilities.



7.2.3 ✓

Required privileges are approved by authorized personnel



7.2.4 ✓

All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows:

- At least once every six months.
- To ensure user accounts and access remain appropriate based on job function.
- Any inappropriate access is addressed.
- Management acknowledges that access remains appropriate.

Thank you for your attention to this matter. I look forward to your response and to resolving this issue in accordance with our obligations.

Exhibit 19J

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

Exhibit 19K

From:	**Ryan Wagner**
Sent:	**Tuesday, May 21, 2024 5:37 PM**
To:	**Glenn Norris**
Cc:	**Justin Drummond; Rich Hartman; Karen Debus; Matt Norris**
Subject:	**Re: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS**

Thank you for your response. I will send Ryan Brooks the link to complete the PCI DSS 4.0 training and ensure he begins the required processes immediately. However, I must reiterate that reinstating his access without him having completed these steps will place us in violation of PCI DSS 4.0 compliance requirements.

Immediate Actions:

1. Ryan Brooks can choose any available training program as long as we receive proof of completion. Previously, I offered to sit down with him to ensure he understands the necessary information, but under duress, I am not comfortable doing this because of the ongoing threats and pressure, which I am afraid will continue until I certify him regardless of his actual compliance.

2. Restore Access Under Duress: I will reinstate his access as per your directive. This action is being taken under duress and against my professional judgment due to the compliance risks involved.

I must inform you that I am experiencing severe stress and anxiety due to this situation, including a panic attack and hyperventilation throughout this conversation. I am currently shaking badly and struggling to finish this email. If I am unable to complete this task by 9 am tomorrow, it is because I have gone catatonic from this experience. Please understand that I am doing my best under these circumstances.

I strongly advise documenting this decision and the associated risks to protect the company and ourselves. I have also reached out to Geoff VanMaastricht to seek his assistance in finding a long-term solution that ensures compliance.

Thank you for your understanding.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

Exhibit 19K

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093

www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 5:28 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: RE: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

Send Ryan Brooks the Link to complete the PCI DSS 4.0 training and processes. I still want his access returned immediately.

Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 5:13 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: Re: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

I acknowledge your directive and understand the urgency of the situation. However, I must reiterate the compliance risks associated with reinstating Ryan Brooks' access without him completing the necessary PCI DSS 4.0 training and processes.

As the head of IT, my primary responsibility is to ensure that we maintain compliance with all regulatory standards. Restoring Ryan's access without meeting these requirements places our PCI DSS 4.0 certification and the company at significant risk. While I am prepared to follow your instructions, I must stress that this action is being undertaken under duress due to your explicit directive.

Exhibit 19K

I have reached out to Geoff VanMaastricht, our head of corporate security, to seek his assistance in finding a solution that balances our compliance obligations with your request. Here is the email I sent to him, which includes you and President Justin Drummond in the loop:

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner Ryan.Wagner@ohanagp.com
Sent: Tuesday, May 21, 2024 5:09 PM
To: Geoff VanMaastricht Geoff.VanMaastricht@pfhq.com
Cc: Glenn Norris glenn@ohanagp.com; Justin Drummond Justin.Drummond@ohanagp.com
Subject: SAQ - PCI Compliance: We need your assistance

@Geoff VanMaastricht, Would you be available for a meeting tomorrow to discuss this and related PCI Compliance concerns? I am being told to reinstate the same person, but they refuse to do the training, take part in the code review, change control, or any other process to maintain compliance. I don't know what to do and could use your assistance to find a solution that works for our CFO as well as meet the compliance requirements.

To mitigate these risks and protect our compliance standing, I propose the following steps:

Immediate Compliance Training: Expedite Ryan's PCI DSS 4.0 compliance training and ensure it is completed as a top priority.
Temporary Limited Access: Provide Ryan with limited access necessary for immediate tasks, under close monitoring, until he completes the required training and processes.
Documented Agreement: Document this course of action, including the acknowledgment that this decision is made under duress, to protect both the company and ourselves, ensuring we have a record of our compliance efforts and the rationale behind these decisions.
I am available to discuss this further and facilitate any immediate actions required to address your concerns while maintaining our compliance obligations.

Please let me know how you would like to proceed.

Best regards,

This message may include text created with the help of natural language processing.

Book time to meet with me

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 5:05 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>

Exhibit 19K

Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: RE: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

Rich, please prepare a write up for me .

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 5:02 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: Re: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

@Glenn Norris

Thank you for your prompt response. I understand the urgency of your request, but I must reiterate the compliance requirements and potential risks involved in reinstating Ryan Brooks' access without completing the necessary PCI DSS 4.0 training and processes.

Reinstating his access without compliance would put our certification at risk and could have serious legal and security implications for the company. As the head of IT, I have a responsibility to ensure that we adhere to these standards.

Given the gravity of the situation and your directive, I propose a meeting tomorrow morning with you, myself, and the head of corporate security to discuss how we can address this matter without compromising our compliance obligations. This will allow us to find a solution that meets your needs while safeguarding our compliance and security standards.

Please confirm a suitable time for this meeting.

Thank you for your understanding.

This message may include text created with the help of natural language processing.

Book time to meet with me

Exhibit 19K

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 4:59 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: RE: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

If Ryan Brooks does not have access by tomorrow morning , you will be written up for insubordination. Is that clear? Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 4:56 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: Re: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

Thank you for your email. I understand your concerns and would like to clarify the situation regarding Ryan Brooks' access and our compliance requirements.

Compliance and Access Issues:

Exhibit 19K

Yesterday, I consulted with PFHQ about how to handle situations where personnel had not completed required training. Before I could act on the conversation, Ryan Brooks informed me he didn't have time for a mandatory 15-minute meeting, and he had already stated he couldn't complete the required training or other tasks assigned to him. Consequently, I removed him to resolve the block to completing the SAQ, as instructed by PFHQ.

Overnight Changes:

The compliance issues did not change overnight. What changed was the final decision to remove Ryan after he explicitly refused to engage in critical compliance activities. Reinstating his access today would violate PCI DSS 4.0 standards, as I have already informed the head of corporate security that the compliance issue was resolved by terminating his access.

Performance Concerns:

The issues identified by Matt, as well as numerous concerns raised by the accounting department, reflect the quality of Ryan's work. While being responsive is important, it is more critical to ensure that work aligns with our strategic objectives and compliance requirements and does not result in these problems existing. Since September/October, Ryan's recommendations have moved us further from resolution, as evidenced by the ongoing issues highlighted in Matt's email.

Ryan's inability to complete tasks assigned to him and his mismanagement of resources (e.g., setting up a second AVD environment, doubling costs, ignoring Microsoft's recommendations) demonstrate a lack of alignment with our strategic direction. His actions, including making unauthorized changes, have exacerbated our challenges rather than resolving them.

Historical Context:

From the start of the emergency migration project, Ryan proposed outdated solutions, like reinvesting in an old AC system instead of modernizing our platform. Following my HR complaint in November, you stopped supporting the initial proposal and allowed Ryan to make changes against our needs, often in secret. Before my FMLA leave, you reinstated his access despite my concerns. Since FMLA, you and Ryan have been in charge of the IT department. Recently, you informed me I should no longer step back, allowing me to re-establish control and initiate daily standups and other processes to get the team back on track.

Next Steps:

Given the situation:

Ryan must complete the PCI DSS compliance training and participate in the required processes before his access can be reinstated.
Restoring his access without meeting these requirements would jeopardize our PCI DSS 4.0 compliance.
I am committed to resolving these issues in a manner that upholds our compliance standards and addresses our operational needs. Please review the data, recommendations, and conclusions from Microsoft and our current state of issues, which collectively indicate that Ryan is not currently qualified to manage our cloud environment.

We can review these concerns with the head of corporate security, and if I understand why it must happen today, perhaps I can offer a solution that does not result in PCI compliance issues.

Thank you for your understanding and cooperation.

This message may include text created with the help of natural language processing.

Exhibit 19K

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 4:28 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: RE: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

How was Ryan Brooks allowed access yesterday and not today? What changed overnight, it does not make sense that compliance issues were just discovered and changed overnight.

I do not think your stance flies.

Please do as I have instructed you. He will take the test.

See Matt's reason why we need him. Look at attached email.

Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 3:38 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: Re: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

Exhibit 19K

@Glenn Norris

Thank you for your email. I understand your urgency regarding Ryan Brooks' access and want to ensure we handle this appropriately while maintaining our compliance with PCI DSS 4.0 standards.

1. Mandates and Requirements:

   - PFHQ mandates compliance with PCI DSS 4.0, which outlines the specific requirements for all personnel with access to sensitive data and systems. This includes mandatory training and participation in key security processes.

2. Attestation Filings:

   - PFHQ instructed me to complete the attestation filings, which are necessary to certify our compliance with PCI DSS 4.0. These filings were submitted to our compliance auditors and relevant regulatory bodies to confirm that we meet all required security standards.

3. Ryan Brooks' Access:

   - Restoring Ryan Brooks' access without him completing the required training and participating in mandated security processes would violate our PCI DSS 4.0 compliance. This could jeopardize our certification and the security of our systems.

Could you please clarify the consequences you foresee if we do not restore Ryan’s access today? Understanding your concerns will help us address them while ensuring we remain compliant with PCI DSS 4.0 standards.

I must emphasize that compliance with these standards is critical to our operations and security. I am committed to resolving this situation as quickly as possible within the bounds of our compliance requirements.

Please let me know how you would like to proceed, and we can work together to find a solution that maintains our compliance and addresses your needs.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

“Culture eats strategy for breakfast”

Exhibit 19K

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 3:26 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: RE: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

1. Please explain who is mandating this and what it entails.
2. Stop filing attestation filings- who gets these and why were they sent in the last 24 hours?
3. I WANT RYAN'S ACCESS RESTORED TODAY. CONFIRM WHEN THIS IS COMPLETED

Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 2:08 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: Re: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

@Glenn Norris I hope this message finds you well. I appreciate your prompt response regarding Ryan Brooks' compliance and performance. I would like to address the points you raised to ensure clarity and alignment with our compliance requirements and performance expectations.

Compliance Allegations:
Regarding the compliance allegations, it is crucial to clarify that all team members, including vendors, must complete the required PCI DSS compliance training. This is a non-negotiable requirement to maintain our certification and ensure our systems' security and integrity. If Ryan was previously informed that he did not need to complete this training, that was incorrect, and I appreciate his willingness to rectify this.

Compliance Training Requirement:
Ryan must complete the PCI DSS compliance training before he can resume any work, as our attestation has already been filed.
Additional Compliance Requirements:

Beyond the training, Ryan's access has been restricted due to his lack of participation in several PCI DSS-required processes. These include:

Exhibit 19K

Participation in daily standup meetings
Involvement in the change control review board
Engagement in the pipeline for code publishing
Adherence to other necessary procedures
Ryan has previously refused to engage in these processes, which are critical for maintaining our compliance. Additionally, the partial work he has completed has not met PCI DSS compliance standards, and I have had to redo this work to align with our requirements.

Access and Admin Rights:
Regarding your directive to restore Ryan's admin rights immediately, I must emphasize that any such action must comply with our PCI DSS 4 standards. Until Ryan completes the required compliance steps and demonstrates his understanding of PCI DSS requirements, he will not be able to make changes to any system as an administrator. This includes both his software engineer responsibilities and sufficient training for administration.

Next Steps:

Ryan must complete the PCI DSS compliance training immediately.HE IS DOING THIS
Ryan must participate in all PCI DSS required processes, including daily standups, change control review boards, and code publishing pipelines. I DO NOT AGREE
After Ryan completes the training and engages in these processes, we need detailed information on the specific tasks you want him to perform. This will allow us to assign him the least privileged access necessary to maintain PCI compliance.

If you feel it would be helpful, I am open to arranging a meeting with the corporate head of security to weigh in on these items and provide additional perspective on maintaining our compliance and security standards. NO THANK YOU

Thank you for your understanding and cooperation in ensuring we maintain our compliance and security standards. I look forward to resolving this matter collaboratively. I DO NOT AGREE WITH YOUR POSITIONS

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

Exhibit 19K

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 1:48 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>; Glenn Norris <glenn@ohanagp.com>
Subject: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

Ryan, I do not agree with your performance and compliance allegations of Ryan Brooks. I asked him if he was required by you to complete the compliance PCI tests and he was adamant that you stated months ago that he did not need to complete this. He is willing to do it. This is straight from Ryan Brooks.

Regarding his performance, we need to have a conversation on your expectations and role for BC/RB. In my opinion, he has been and still is a valued vendor for our IT needs .

Please ask Justin, Rich, Matt or Karen(and others) how they do or do not value his contribution to our IT needs.

As I stated in our call earlier today, I want his admin rights restored today. There was no discussion with me about this action – I do not approve.

SEE COMMENTS IN RED BELOW

Thank you, Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 1:16 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>
Subject: Ryan Brooks - More Info Needed

@Glenn Norris, I hope you're doing well. I am seeking clarification regarding your directive to retain Ryan Brooks in the IT Department. When we talked today, you expressed a specific need for his services, despite my concerns about his performance and our compliance requirements.

In addition, As part of our compliance with PCI DSS 4 standards, which I recently certified after significant efforts, every team member must meet the requirements. Ryan Brooks' refusal to follow proper procedures and complete

Exhibit 19K

the required upskill training posed a substantial obstacle to maintaining PCI DSS 4 unless he is able to do the things that I have required of him.

To clarify:

1. Security Training: Ryan has not completed the mandatory security training, which disqualifies him from being employed as a software engineer under PCI DSS 4 standards. HE WILL DO THIS IF IT IS REQUIRED.

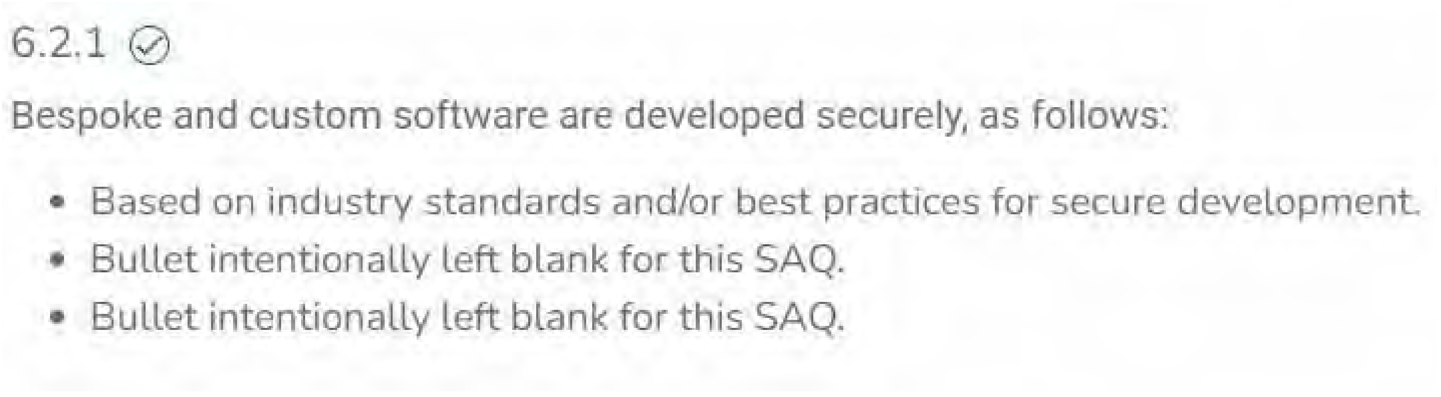
2. Code Review Process: He has been unable to participate in the code review process, making him unsuitable for automation or SQL work. WHAT IS THE REQUIRED TIME INVESTMENT HERE?

3. Change Control Review Board: Ryan's lack of participation in the change control review board precludes him from performing any sysadmin tasks or handling M365 or Azure responsibilities. HE HAS BEEN ON EVERY TUESDAY 230 CALL AND YOU GHOSTED THAT CALL ON 5-7-24 AND HE WAS IN ATTENDANCE. HE WILL NOT BE ON TODAY'S CALL SINCE YOU INADVERTANTLY FIRED HIM YESTERDAY.

Given these compliance issues, retaining Ryan to work in these areas conflicts with the PCI DSS 4 standards. His non-compliance and refusal to adhere to required protocols undermine our efforts to maintain these critical standards.

Please provide specific details regarding the necessity of retaining Ryan's services and ensure that it does not conflict with our PCI DSS 4 compliance requirements. I would like you to know that understanding your rationale and how it aligns with these standards is essential for moving forward.

Thank you for your attention to this matter. I look forward to your response to resolve this issue in compliance with our obligations.

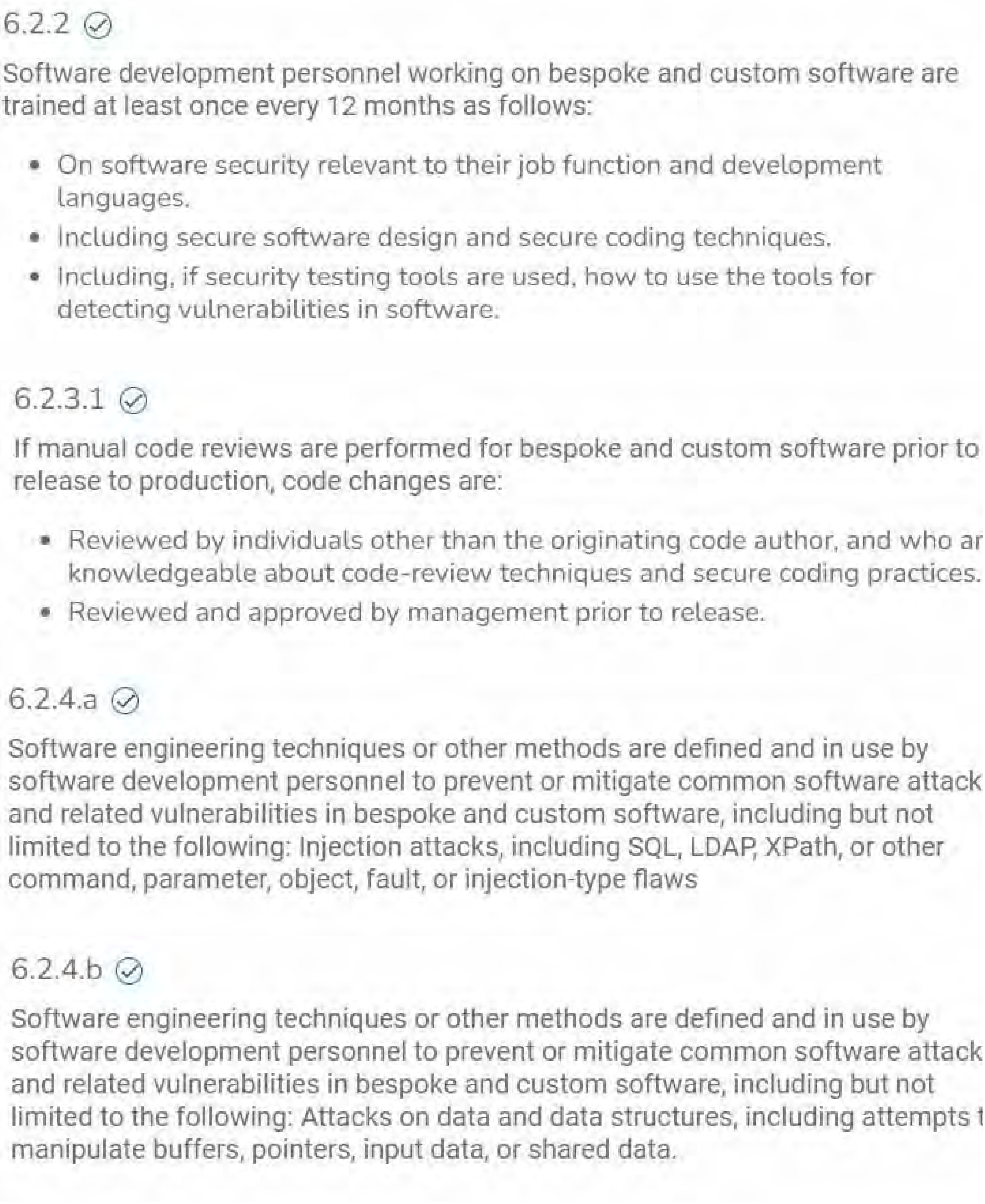


6.2.1 ✓

Bespoke and custom software are developed securely, as follows:

- Based on industry standards and/or best practices for secure development.
- Bullet intentionally left blank for this SAQ.
- Bullet intentionally left blank for this SAQ.

Exhibit 19K



6.2.2 ✓

Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows:

- On software security relevant to their job function and development languages.
- Including secure software design and secure coding techniques.
- Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.

6.2.3.1 ✓

If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are:

- Reviewed by individuals other than the originating code author, and who ar knowledgeable about code-review techniques and secure coding practices.
- Reviewed and approved by management prior to release.

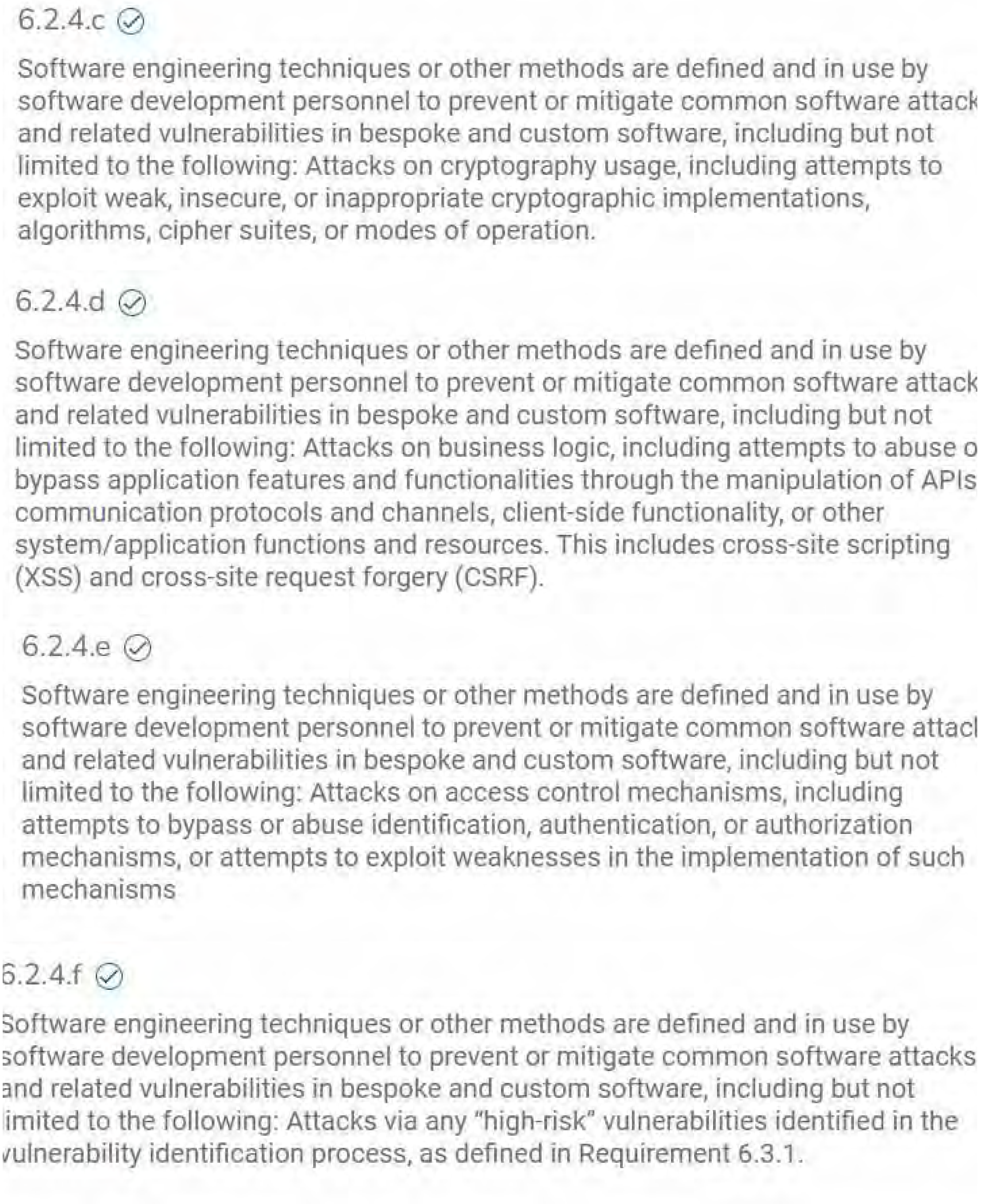
6.2.4.a ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws

6.2.4.b ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on data and data structures, including attempts t manipulate buffers, pointers, input data, or shared data.

Exhibit 19K



6.2.4.c ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation.

6.2.4.d ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on business logic, including attempts to abuse o bypass application features and functionalities through the manipulation of APIs communication protocols and channels, client-side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF).

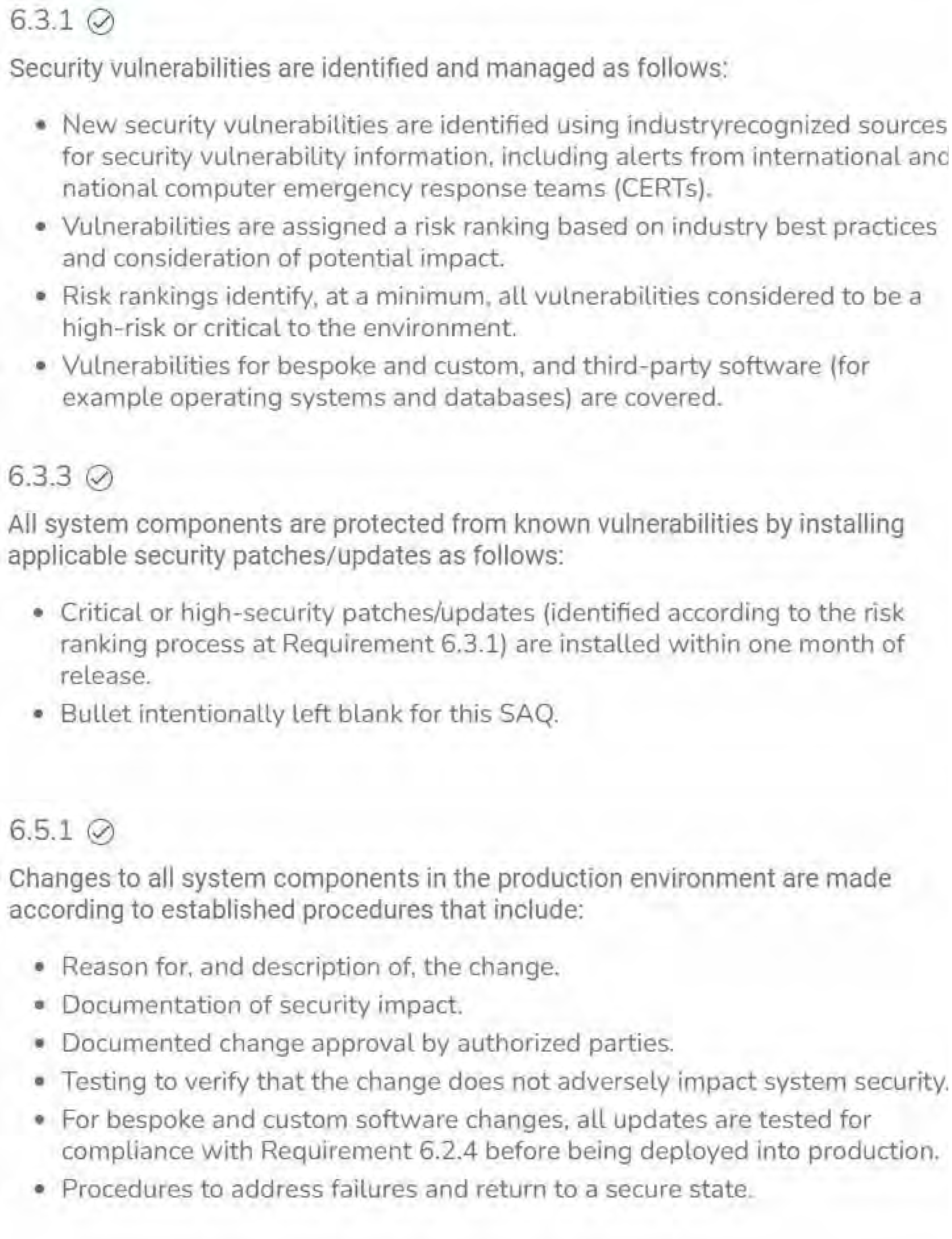
6.2.4.e ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms

6.2.4.f ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks via any “high-risk” vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1.

Exhibit 19K



6.3.1 ✓

Security vulnerabilities are identified and managed as follows:

- New security vulnerabilities are identified using industryrecognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).
- Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.
- Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.
- Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.

6.3.3 ✓

All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows:

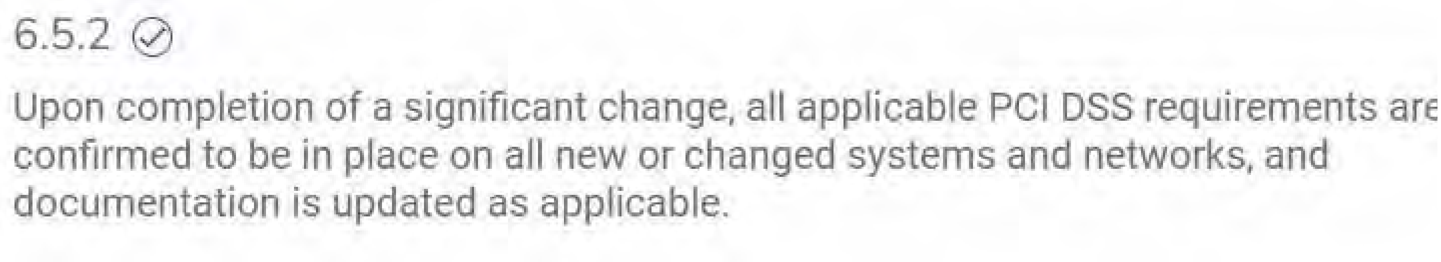
- Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release.
- Bullet intentionally left blank for this SAQ.

6.5.1 ✓

Changes to all system components in the production environment are made according to established procedures that include:

- Reason for, and description of, the change.
- Documentation of security impact.
- Documented change approval by authorized parties.
- Testing to verify that the change does not adversely impact system security.
- For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production.
- Procedures to address failures and return to a secure state.

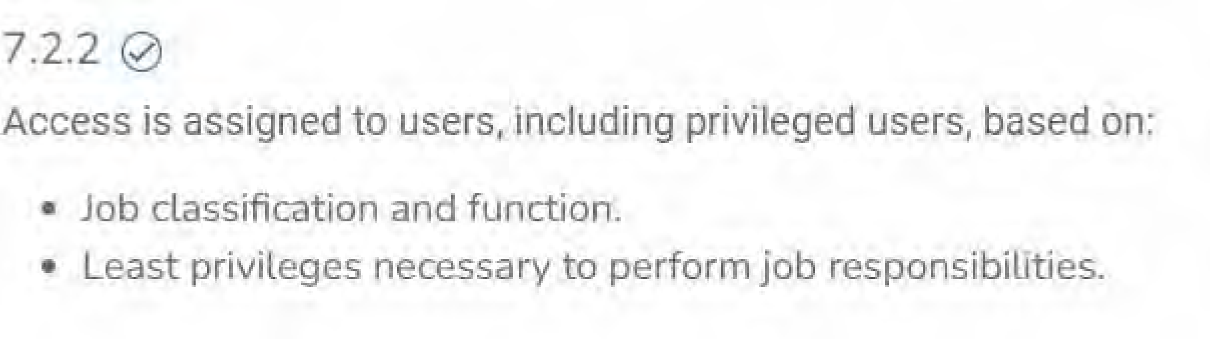
Exhibit 19K



6.5.2 ✓

Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.

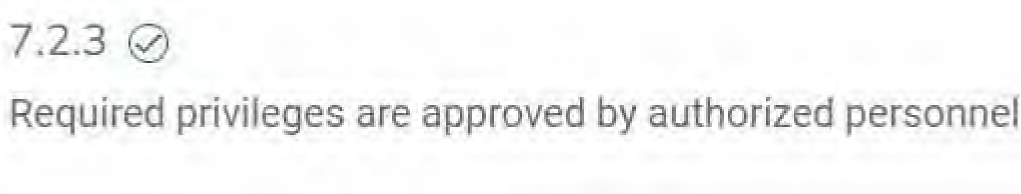
Please provide specific details regarding the necessity of retaining Ryan's services which does not conflict with our PCI DSS 4 compliance requirements. I would like you to know that understanding your rationale and how it aligns with these standards is essential for moving forward by assigning him permissions that will give him the least privileges necessary while not performing tasks listed above or otherwise in the PCI DSS 4.



7.2.2 ✓

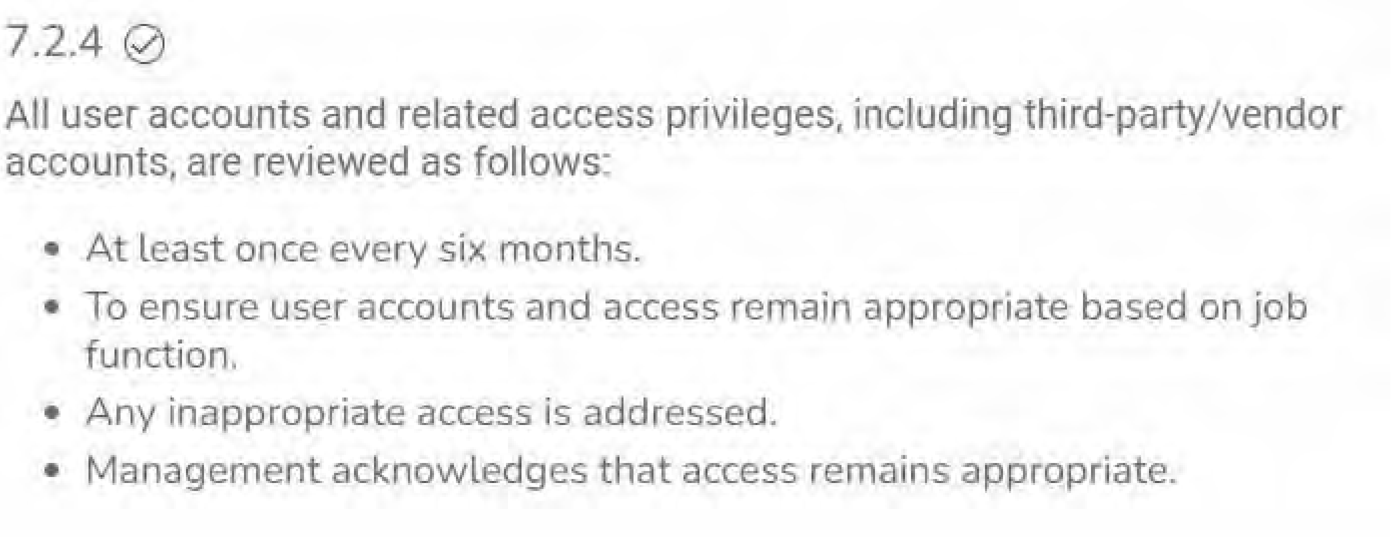
Access is assigned to users, including privileged users, based on:

- Job classification and function.
- Least privileges necessary to perform job responsibilities.



7.2.3 ✓

Required privileges are approved by authorized personnel



7.2.4 ✓

All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows:

- At least once every six months.
- To ensure user accounts and access remain appropriate based on job function.
- Any inappropriate access is addressed.
- Management acknowledges that access remains appropriate.

Thank you for your attention to this matter. I look forward to your response and to resolving this issue in accordance with our obligations.

Exhibit 19K

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

“Culture eats strategy for breakfast”

Exhibit 19L

Ryan Dillon-Capps

From:	**Ryan Wagner**
Sent:	**Tuesday, May 21, 2024 6:00 PM**
To:	**Ryan Brooks BC**
Cc:	**Justin Drummond; Glenn Norris; Rich Hartman; Karen Debus; Matt Norris**
Subject:	**PCI DSS 4 Training**

Glenn has told me to give you options for the developer course work. You do not need to choose one of these. You can choose any course for developers that has a completion certificate or similar output.

Course Name	Provider	Role Suited For	Time to Complete	Mode	Cost
PCI DSS Security - Application Security	Synopsys	Developers, DevOps	Varies	Online	Contact for price
PCI Secure Coding Training Requirements	PCI DSS Guide	Developers	Varies	Online	Varies
Mastering PCI DSS v4: Comprehensive Compliance Unlocked	Udemy	Developers	5 hours	Online	$100
PCI DSS Compliance Masterclass	Udemy	Developers	8 hours	Online	$150
PCI DSS 4.0 for Developers	Pluralsight	Developers	4 hours	Online	Subscription
PCI DSS for Developers	Secure Ideas	Developers	2 days	Online	$1200
PCI DSS Secure Coding Practices	ISACA	Developers	3 days	Online	$2000
PCI DSS Implementation and Coding Guidelines	BSI Group	Developers	2 days	Online	$1200
PCI DSS Developer Training	Learning Tree	Developers	3 days	Online	$2000
PCI DSS Compliance for Software Developers	Coursera	Developers	10 hours	Online	$100/month
PCI DSS Awareness and Secure Coding	ACI Learning	Developers	2 hours	Online	$100
PCI DSS for Application Security	SANS Institute	Developers	2 days	Online	$1000
PCI DSS Software Development Compliance	InfoSec Institute	Developers	5 days	Online	$3000
PCI DSS Coding Standards and Compliance	Trainocate	Developers	3 days	In-person	$1800
PCI DSS: Building Secure Software	Skillsoft	Developers	5 hours	Online	Subscription
PCI DSS Secure Coding Practices	Simplilearn	Developers	Self-paced	Online	$200
PCI DSS Development and Compliance	Trustwave	Developers	2 days	Online	$1500
PCI DSS Secure Software Lifecycle	PCI Security Standards	Developers	Varies	Online	Contact for price
PCI DSS Implementation for Software Engineers	IT Governance	Developers	3 days	Online	$1500
PCI DSS Secure Software Development	Cybrary	Developers	6 hours	Online	$99/year

Exhibit 19L

Also, here are courses to help you prepare to support us as an administrator or engineer.

Course Name	Provider	Role Suited For	Time to Complete	Mode	Cost
PCI DSS Secure Coding Practices	ISACA	Engineers	3 days	Online	$2000
PCI DSS Implementation for Software Engineers	IT Governance	Engineers	3 days	Online	$1500
PCI DSS Development and Compliance	Trustwave	Engineers	2 days	Online	$1500
PCI DSS Secure Software Lifecycle	PCI Security Standards	Engineers	Varies	Online	Contact for price
PCI DSS Secure Software Development	Cybrary	Engineers	6 hours	Online	$99/year
PCI DSS Software Development Compliance	InfoSec Institute	Engineers	5 days	Online	$3000
PCI DSS: Building Secure Software	Skillsoft	Engineers	5 hours	Online	Subscription
PCI DSS 4.0 for Engineers	Pluralsight	Engineers	4 hours	Online	Subscription
PCI DSS for Developers	Secure Ideas	Engineers	2 days	Online	$1200
PCI DSS Awareness and Secure Coding	ACI Learning	Engineers	2 hours	Online	$100

Course Name	Provider	Role Suited For	Time to Complete	Mode	Cost
PCI DSS Compliance Masterclass	Udemy	Administrators	8 hours	Online	$150
Internal Security Assessor Training	PCI Security Standards	Administrators	5 days	Online	$3000
PCI DSS: Protecting Cardholder Data	LinkedIn Learning	Administrators	1 hour	Online	$30/month
PCI DSS Implementation and Compliance	BSI Group	Administrators	2 days	Online	$1200
PCI DSS Compliance for IT Administrators	Pluralsight	Administrators	4 hours	Online	Subscription
PCI DSS Awareness Training	PCI Security Standards	Administrators	1 day	Online	$500
PCI DSS for IT Professionals	Udemy	Administrators	8 hours	Online	$150
PCI DSS Implementation Training	Learning Tree	Administrators	3 days	Online	$2000
PCI DSS Internal Security Assessor (ISA)	PCI Security Standards	Administrators	3 days	In-person	$2000
PCI DSS Administration and Management	Coursera	Administrators	10 hours	Online	$100/month

We will also need you to participate in the relevant meetings that aim to satisfy the PCI DSS 4 requirements, which are significantly more extensive than previously. I believe you will understand what I speak of as you complete the relevant courses. I suspect that administrator and engineer courses contain relatively similar information. You

Exhibit 19L

being software qualified every 12 months is required. The admin and engineering are here to help you understand why we are doing these meetings and why we are making some of the decisions that we are making.

We have lots of work to do because in roughly 12 months, the PCI DSS 4 will be adding many new requirements, and we are barely scrapping by today with me doing excessive hours again to get us through the SAQ today. Not performing the tasks assigned in a timely manner has not been nor will it be acceptable. Please note that this action has been taken under duress and triggered my PTSD symptoms severely, which may delay the time to make the changes as I put in some safeguards to prevent tampering.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093

www.planetfitness.com

"Culture eats strategy for breakfast"

Exhibit 19M

From:	**Ryan Wagner**
Sent:	**Tuesday, May 21, 2024 6:27 PM**
To:	**Glenn Norris**
Cc:	**Justin Drummond; Rich Hartman; Karen Debus**
Subject:	**Re: REPEAT QUESTION - PCI DSS 4 Compliance Training**

1. **Regarding Ryan Brooks:**

   - **Role**: Ryan is the only one creating custom software solutions for us.
   - **Attendance**: He is not attending meetings or participating in the process.
   - **Actions**: He is implementing changes without my knowledge that may not comply with the requirements.

When I assigned training to everyone, I told them that I would restrict their duties if necessary.

Geoff contacted me yesterday as a follow-up to an email from last week.

As with the first bullet point, here is the requirement. This is not the same requirement that the other people on the team have because no one else is building custom software for us, but if they were then they would need to meet this same requirement.

I find it odd that you constantly disagree and do not believe me, and my reply is --- let's go ask an expert. An investigator, a lawyer, and the head of corporate security. If I am wrong, then they would be the ones to tell us, and there would not be any issues. I do not understand why we don't do this on any of these topics; it has to be easier than this. You might not be in physical pain right now because of this and suffering from today, but I am and I don't deserve this. You never disagree with me – you disagree with the data, the math, the analytics, the experts, the manufacturers, and the company who wrote the OS and software, and all I ever do is show you what they said. What the data says. What the math says. What the analysis says. Or even just asking the question - why is this number so low? Why did we submit a number to the bank that was half what the invoices showed when we went through them one by one. Why did Rich immediately tell you and the 2 Cs that I filed an HR complaint about? Why are my role and responsibilities being stripped away? Why can't you let me do my job? when do I get to do my job?

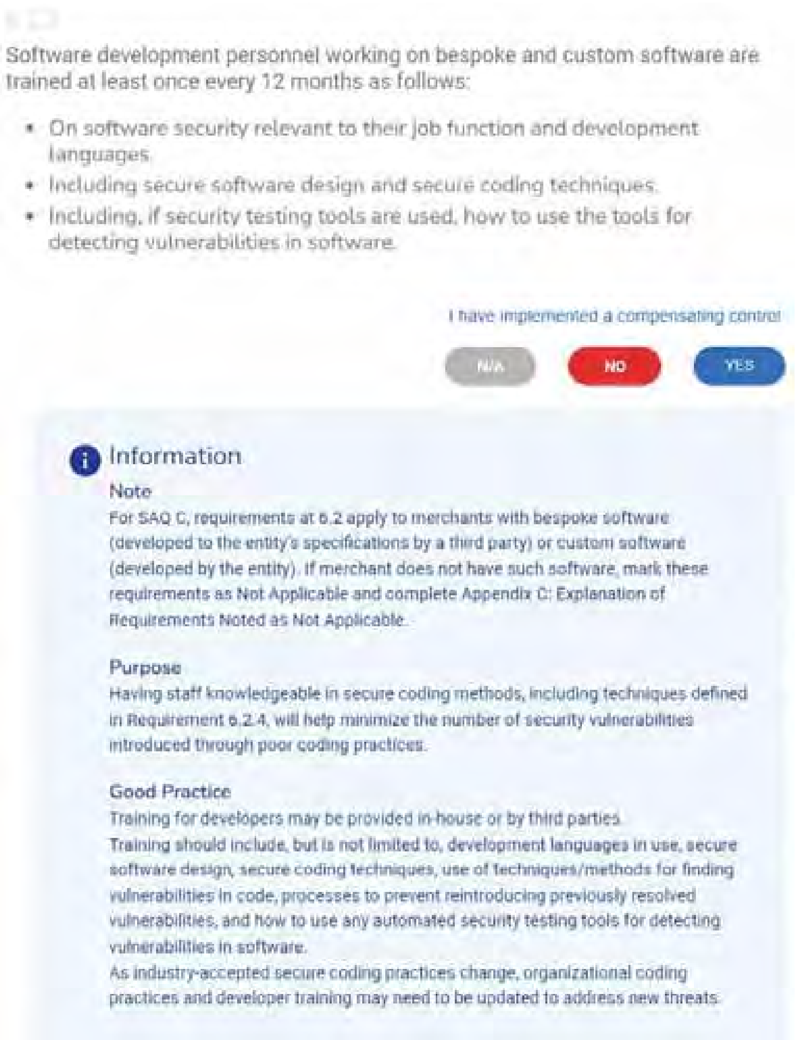
Are you forcing me under duress to give Ryan Brooks access when the reason I could answer yes to this was because I removed him from the system and he can no longer make changes? I know that you said Yes do this or get written up.

I showed you what it said... you said you disagree --- with --- the PCI DSS 4 requirements? You don't disagree with me because I never said something to disagree with.

I don't deserve this... this is my opinion. I don't deserve to be treated like this. I don't deserve to be told that I use too many words and am too professional because I don't swear. I don't deserve to be made to feel like my greatest weakness is that I am not enough of "a man". well, I am not --- I am non-binary. I don't talk like you because I am not like you. I do however believe that I embody everything this company says they stand for, and for months I

Exhibit 19M

have tried to convince you to listen to an expert before your actions are seen in a manner that causes you to end up in an orange jump suit. The more I try to prevent you from making decisions with the potential for serious consequences you attack and attack and attack. I don't deserve this... those are my opinions and you are free to disagree



Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows:

- On software security relevant to their job function and development languages.
- Including secure software design and secure coding techniques.
- Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.

I have implemented a compensating control

Information

Note

For SAQ C, requirements at 6.2 apply to merchants with bespoke software (developed to the entity's specifications by a third party) or custom software (developed by the entity). If merchant does not have such software, mark these requirements as Not Applicable and complete Appendix C: Explanation of Requirements Noted as Not Applicable.

Purpose

Having staff knowledgeable in secure coding methods, including techniques defined in Requirement 6.2.4, will help minimize the number of security vulnerabilities introduced through poor coding practices.

Good Practice

Training for developers may be provided in-house or by third parties.

Training should include, but is not limited to, development languages in use, secure software design, secure coding techniques, use of techniques/methods for finding vulnerabilities in code, processes to prevent reintroducing previously resolved vulnerabilities, and how to use any automated security testing tools for detecting vulnerabilities in software.

As industry-accepted secure coding practices change, organizational coding practices and developer training may need to be updated to address new threats.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093

www.planetfitness.com

"Culture eats strategy for breakfast"

Exhibit 19M

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 5:59 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Glenn Norris <glenn@ohanagp.com>
Subject: REPEAT QUESTION - PCI DSS 4 Compliance Training

Ryan, I asked you this question yesterday with no response. Please answer this question. Did everyone listed below take their course except Ryan Brooks?

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Monday, May 20, 2024 3:05 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>
Subject: Re: PCI DSS 4 Compliance Training

Yes - Geoff is the head of IT security at PFHQ. This set of questions applies to Ryan Brooks for the work he does for us with our custom software solutions.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

Exhibit 19M

From: Glenn Norris <glenn@ohanagp.com>
Sent: Monday, May 20, 2024 2:06 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>
Subject: RE: PCI DSS 4 Compliance Training

Ryan, is Geoff from Corp? If so, are they requiring us to complete PCI Standards on line? Did everyone listed below take their course except Ryan Brooks?

Let's discuss.

Thank you, Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

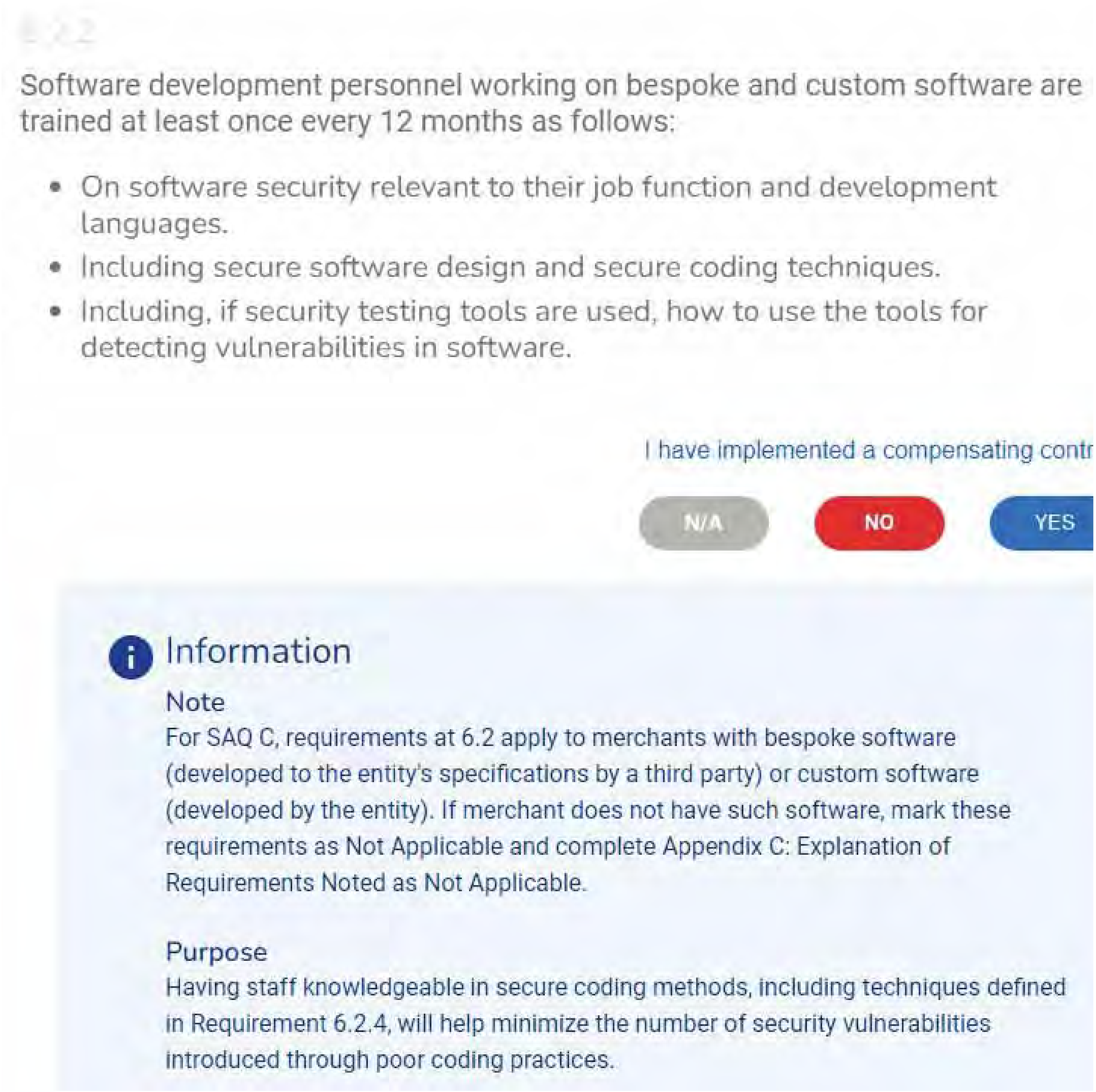
office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Monday, May 20, 2024 1:34 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>
Subject: Re: PCI DSS 4 Compliance Training

@Glenn Norris I got Geoff asking if we can wrap up our assessment for DSS4. We are still stuck on the training requirement for RB because he doesn't have time to complete the required PCI training. What would you like to do about this?

Exhibit 19M



6.2.2

Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows:

- On software security relevant to their job function and development languages.
- Including secure software design and secure coding techniques.
- Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.

Information

Note

For SAQ C, requirements at 6.2 apply to merchants with bespoke software (developed to the entity's specifications by a third party) or custom software (developed by the entity). If merchant does not have such software, mark these requirements as Not Applicable and complete Appendix C: Explanation of Requirements Noted as Not Applicable.

Purpose

Having staff knowledgeable in secure coding methods, including techniques defined in Requirement 6.2.4, will help minimize the number of security vulnerabilities introduced through poor coding practices.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

Exhibit 19M

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Thursday, March 21, 2024 5:03 PM
To: Ryan Brooks BC <rb@baltimoreconsulting.com>; Darren Koritzka <Darren.Koritzka@ohanagp.com>; Dante Martinez <dante.martinez@ohanagp.com>; Rikki Francisco <rikki.francisco@ohanagp.com>; Ann Pinera <Mareann.Pinera@ohanagp.com>; Glenn Norris <glenn@ohanagp.com>
Subject: PCI DSS 4 Compliance Training

By March 31, 2024, I need everyone to complete their assigned training. I understand this is short notice, and if you are unable to meet this deadline, please let me know when you can. After Mary 31, 2024, we may need to augment your responsibility if this is not completed.

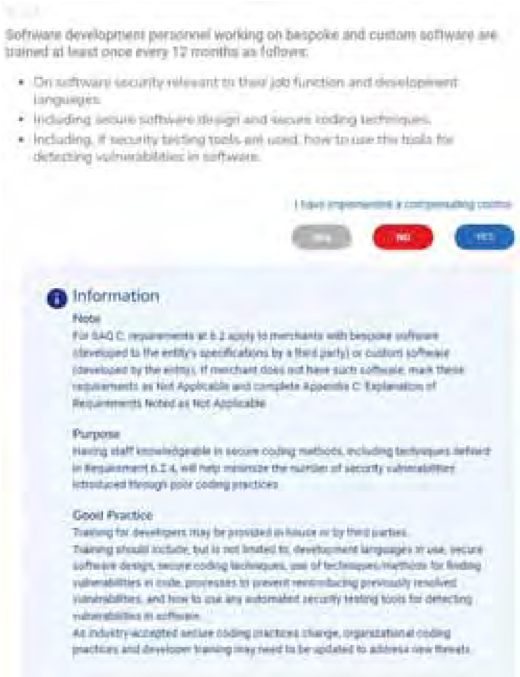
@Darren Koritzka @Dante Martinez @Rikki Francisco @Ann Pinera
Payment Card Industry (PCI) Data Security Standard (DSS) - Microsoft Compliance | Microsoft Learn
Review all the files in the PCI_DSS_QRG-v4.zip attachment

@Darren Koritzka @Dante Martinez @Ryan Brooks BC You also have
Best practices for the Microsoft identity platform - Microsoft identity platform | Microsoft Learn
Microsoft Entra ID and PCI-DSS Requirement 6 - Microsoft Entra | Microsoft Learn

@Ryan Brooks BC @Rikki Francisco @Ann Pinera You also have
Review all the files in the PCI-Secure-Software-Program

Do you need to remember 100% of this material, but here are some key takeaways:
@Ryan Brooks BC You have the highest level of PCI compliance requirement because you work onbespon bespokeoke software for us, and I need an exact date from you when you have completed this task because I am going to attest that you have affirmed to me compliance training on that date. You need to understand the following concepts:

Exhibit 19M



6.2.2

Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows:

- On software security relevant to their job function and development languages.
- Including secure software design and secure coding techniques.
- Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.

I have implemented a compensating control

Information

Note

For SAQ C, requirements at 6.2 apply to merchants with bespoke software (developed to the entity's specifications by a third party) or custom software (developed by the entity). If merchant does not have such software, mark these requirements as Not Applicable and complete Appendix C: Explanation of Requirements Noted as Not Applicable.

Purpose

Having staff knowledgeable in secure coding methods, including techniques defined in Requirement 6.2.4, will help minimize the number of security vulnerabilities introduced through poor coding practices.

Good Practice

Training for developers may be provided in-house or by third parties.

Training should include, but is not limited to, development languages in use, secure software design, secure coding techniques, use of techniques/methods for finding vulnerabilities in code, processes to prevent reintroducing previously resolved vulnerabilities, and how to use any automated security testing tools for detecting vulnerabilities in software.

As industry-accepted secure coding practices change, organizational coding practices and developer training may need to be updated to address new threats.

I will need to "interview" you afterwards or you can provide the certification of a completed PCI DSS 4 software developer course. I will be using questions based on the PCI Compliance assessment that follows this question. You should be comfortable speaking about bugs, flaws, exploits, attacks and how to detect, prevent, test for, and remediate/resolve. You should understand concepts like CERTs and FIRST as a developer who has externally accessible applications inclusive of ones that are directly on a PCI compliant network and are used to input PCI data for transmission to a processor.

@Ryan Brooks BC @Darren Koritzka @Dante Martinez
You have a smaller scope of impact. Patch management, change control procedures, change control documentation and CERT and FIRST concepts. Focus on detection of exploits as they would impact your respective domains and become familiar with how we track zero day attacks and what we should do once they are made aware to us.

@Ann Pinera @Rikki Francisco @Ryan Brooks BC
You have the smallest scope which is focused on bugs that create vulnerabilities and you should understand the software life cycle, from stage to dev to production. Why they exist and what are we doing in those steps to detect and address potential attack vectors from our own code.

@Glenn Norris We should discuss where we feel this could be a need to address with OSI and Gross/Nectari. There is an physical assessment and remote assessment that we would have done by a qualified accessor, but I can tell you now that they will fail. Alternatively, we could require them to pass a certification course to demonstrate by 3rd party they have the required knowledge. Gross/Nectari I could argue never touch anything that could fall under the PCI scope, but that makes one small assumption that I need you/matt to attest to and that is we never in any way have our own credit card information recorded somewhere in any of those sage systems. Not the fragments on a receipt, but anything more should result in a conversation so we can determine our comfort level and we can review the standard as it applies. Most of this will be covered in section 6 if you want to review that or all of it, but please understand that I am attesting to this and I would like that conversation for my own peace of mind.

This message may include text created with the help of natural language processing.

Exhibit 19M

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

“Culture eats strategy for breakfast”

Exhibit 19N

From:	**Ryan Wagner**
Sent:	**Tuesday, May 21, 2024 8:54 PM**
To:	**Glenn Norris**
Cc:	**Justin Drummond; Rich Hartman; Karen Debus**
Subject:	**Re: REPEAT QUESTION - PCI DSS 4 Compliance Training**

@Glenn Norris

I wish I could avoid checking my email right now, as it's not helping the situation. However, I want to address your concerns as clearly as possible.

First, I need to clarify that this is not a moot point. To make an informed decision, you need to ask the right questions, or the answers you get won't be helpful.

One of the false assumptions here is that you are only aware of one of Ryan's solutions and assume this represents the entirety of his work.

Did you know that Ryan also developed the PFHQ-approved Kiosk platform? This platform is deployed on iPads at clubs, allowing users to input payment information directly into the PCI network. Furthermore, this solution is hosted in our Azure environment, which Ryan set up and deployed alone.

Given this information, it's crucial to determine if the AP Processing software developed by Baltimore Consulting has any PCI-compliant information that falls under PCI DSS 4 requirements. If no checking account or other sensitive payment information is involved, then the requirement may be less critical. However, we must thoroughly review all aspects to ensure compliance.

This is one example of where we need to first ask the right questions. In the state I am in, I don't think I can give a complete answer that encompasses every possible way that I have found or still need to look into, but it is something that needs to be done.

I am trying to comply with the mandate set forth, but we need to fully understand the scope of Ryan's involvement and the potential risks to our compliance.

Thank you for your understanding.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

Exhibit 19N

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093

www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 7:42 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>
Subject: RE: REPEAT QUESTION - PCI DSS 4 Compliance Training

The question that I need answered is: Does the software package that Baltimore Consulting Developed for AP Processing have any PCI Compliant relative information that falls under the PCI DSS 4 requirements?

If the information in the AP Software application does not apply, then this requirement becomes mute.

No checking account information is in the software.

Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 6:27 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>
Subject: Re: REPEAT QUESTION - PCI DSS 4 Compliance Training

1. **Regarding Ryan Brooks:**

   - **Role**: Ryan is the only one creating custom software solutions for us.
   - **Attendance**: He is not attending meetings or participating in the process.

Exhibit 19N

- **Actions**: He is implementing changes without my knowledge that may not comply with the requirements.

When I assigned training to everyone, I told them that I would restrict their duties if necessary.

Geoff contacted me yesterday as a follow-up to an email from last week.

As with the first bullet point, here is the requirement. This is not the same requirement that the other people on the team have because no one else is building custom software for us, but if they were then they would need to meet this same requirement.

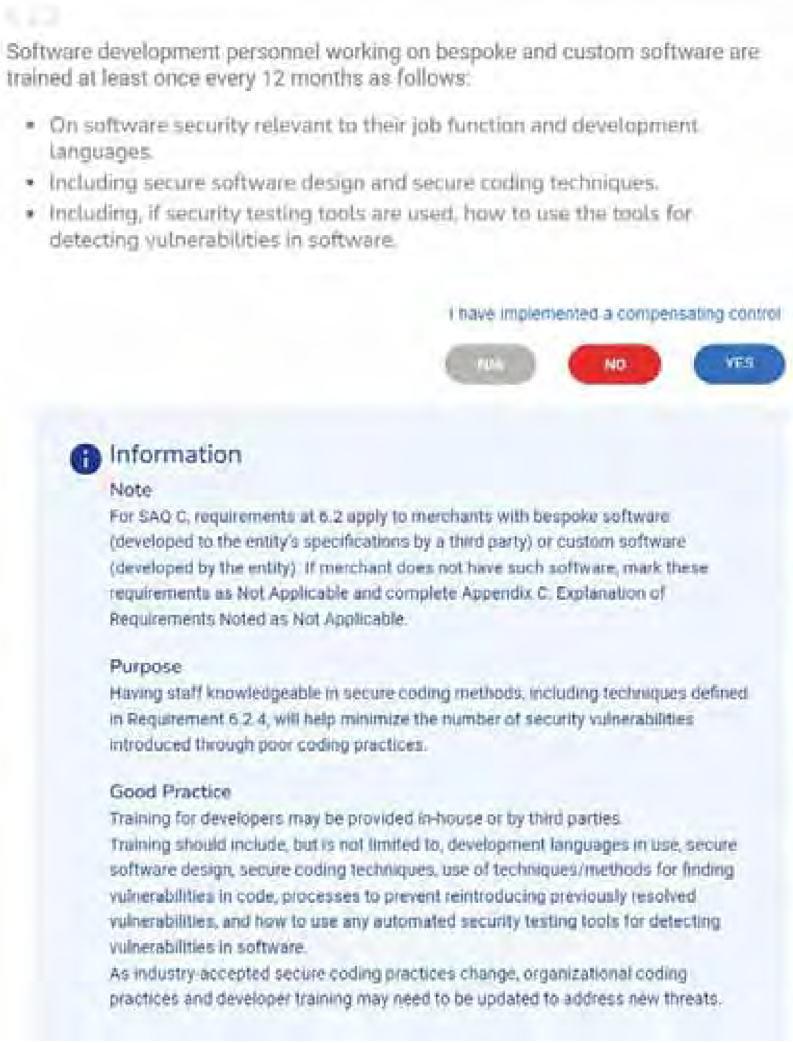
I find it odd that you constantly disagree and do not believe me, and my reply is --- let's go ask an expert. An investigator, a lawyer, and the head of corporate security. If I am wrong, then they would be the ones to tell us, and there would not be any issues. I do not understand why we don't do this on any of these topics; it has to be easier than this. You might not be in physical pain right now because of this and suffering from today, but I am and I don't deserve this. You never disagree with me – you disagree with the data, the math, the analytics, the experts, the manufacturers, and the company who wrote the OS and software, and all I ever do is show you what they said. What the data says. What the math says. What the analysis says. Or even just asking the question - why is this number so low? Why did we submit a number to the bank that was half what the invoices showed when we went through them one by one. Why did Rich immediately tell you and the 2 Cs that I filed an HR complaint about? Why are my role and responsibilities being stripped away? Why can't you let me do my job? when do I get to do my job?

Are you forcing me under duress to give Ryan Brooks access when the reason I could answer yes to this was because I removed him from the system and he can no longer make changes? I know that you said Yes do this or get written up.

I showed you what it said... you said you disagree --- with --- the PCI DSS 4 requirements? You don't disagree with me because I never said something to disagree with.

I don't deserve this... this is my opinion. I don't deserve to be treated like this. I don't deserve to be told that I use too many words and am too professional because I don't swear. I don't deserve to be made to feel like my greatest weakness is that I am not enough of "a man". well, I am not --- I am non-binary. I don't talk like you because I am not like you. I do however believe that I embody everything this company says they stand for, and for months I have tried to convince you to listen to an expert before your actions are seen in a manner that causes you to end up in an orange jump suit. The more I try to prevent you from making decisions with the potential for serious consequences you attack and attack and attack. I don't deserve this... those are my opinions and you are free to disagree

Exhibit 19N



6.2.2

Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows:

- On software security relevant to their job function and development languages.
- Including secure software design and secure coding techniques.
- Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.

I have implemented a compensating control

Information

Note

For SAQ C, requirements at 6.2 apply to merchants with bespoke software (developed to the entity's specifications by a third party) or custom software (developed by the entity). If merchant does not have such software, mark these requirements as Not Applicable and complete Appendix C: Explanation of Requirements Noted as Not Applicable.

Purpose

Having staff knowledgeable in secure coding methods, including techniques defined in Requirement 6.2.4, will help minimize the number of security vulnerabilities introduced through poor coding practices.

Good Practice

Training for developers may be provided in-house or by third parties.

Training should include, but is not limited to, development languages in use, secure software design, secure coding techniques, use of techniques/methods for finding vulnerabilities in code, processes to prevent reintroducing previously resolved vulnerabilities, and how to use any automated security testing tools for detecting vulnerabilities in software.

As industry-accepted secure coding practices change, organizational coding practices and developer training may need to be updated to address new threats.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 5:59 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus

Exhibit 19N

<karen.debus@ohanagp.com>; Glenn Norris <glenn@ohanagp.com>
Subject: REPEAT QUESTION - PCI DSS 4 Compliance Training

Ryan, I asked you this question yesterday with no response. Please answer this question. Did everyone listed below take their course except Ryan Brooks?

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Monday, May 20, 2024 3:05 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>
Subject: Re: PCI DSS 4 Compliance Training

Yes - Geoff is the head of IT security at PFHQ. This set of questions applies to Ryan Brooks for the work he does for us with our custom software solutions.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Monday, May 20, 2024 2:06 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>
Subject: RE: PCI DSS 4 Compliance Training

Exhibit 19N

Ryan, is Geoff from Corp? If so, are they requiring us to complete PCI Standards on line? Did everyone listed below take their course except Ryan Brooks?

Let’s discuss.

Thank you, Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

OHANA
Growth Partners

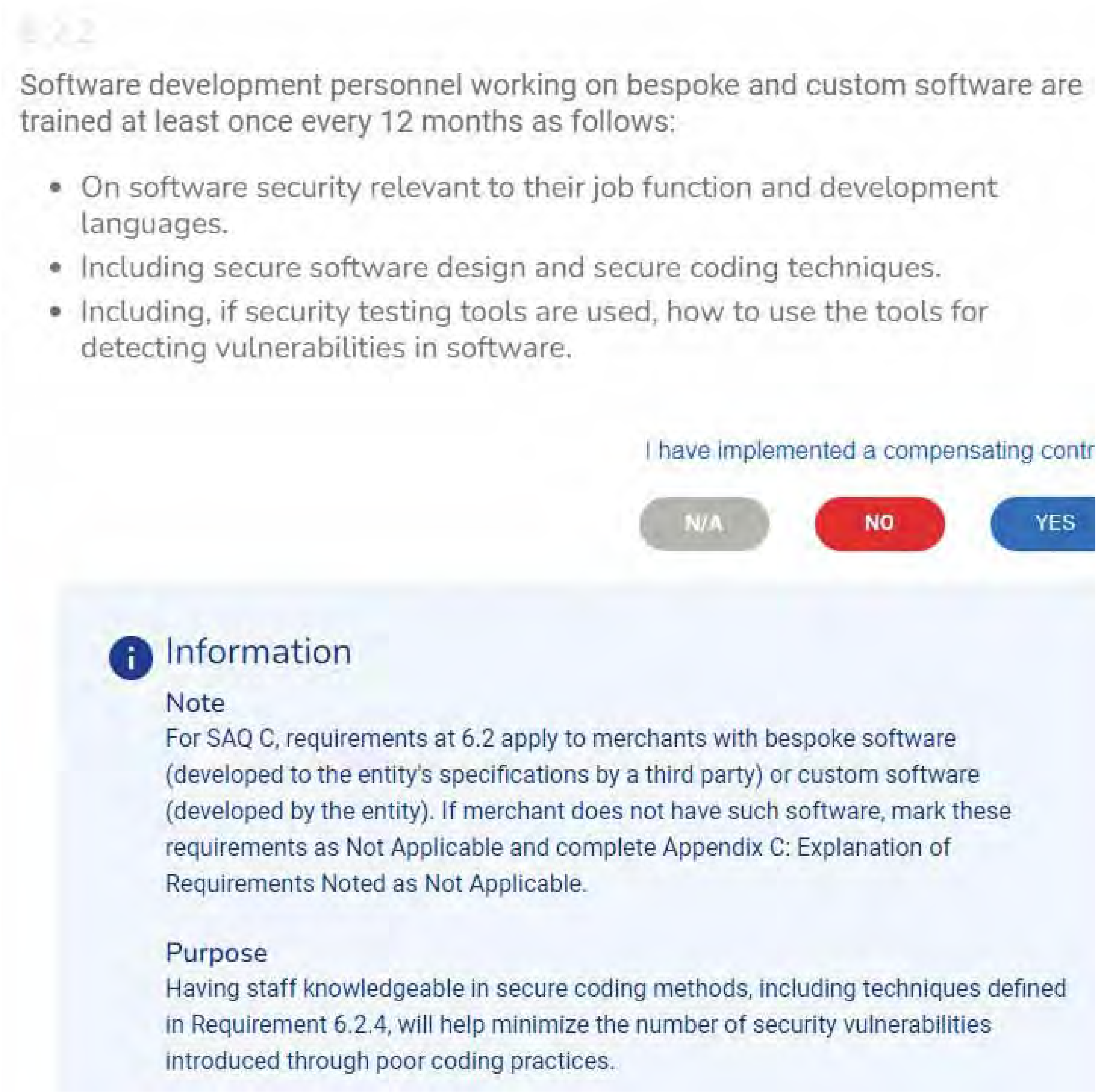
office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

“Culture eats strategy for breakfast”

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Monday, May 20, 2024 1:34 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>
Subject: Re: PCI DSS 4 Compliance Training

@Glenn Norris I got Geoff asking if we can wrap up our assessment for DSS4. We are still stuck on the training requirement for RB because he doesn't have time to complete the required PCI training. What would you like to do about this?

Exhibit 19N



6.2.2

Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows:

- On software security relevant to their job function and development languages.
- Including secure software design and secure coding techniques.
- Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.

I have implemented a compensating contr

Information

Note

For SAQ C, requirements at 6.2 apply to merchants with bespoke software (developed to the entity's specifications by a third party) or custom software (developed by the entity). If merchant does not have such software, mark these requirements as Not Applicable and complete Appendix C: Explanation of Requirements Noted as Not Applicable.

Purpose

Having staff knowledgeable in secure coding methods, including techniques defined in Requirement 6.2.4, will help minimize the number of security vulnerabilities introduced through poor coding practices.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

Exhibit 19N

OHANA
Growth Partners

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Thursday, March 21, 2024 5:03 PM
To: Ryan Brooks BC <rb@baltimoreconsulting.com>; Darren Koritzka <Darren.Koritzka@ohanagp.com>; Dante Martinez <dante.martinez@ohanagp.com>; Rikki Francisco <rikki.francisco@ohanagp.com>; Ann Pinera <Mareann.Pinera@ohanagp.com>; Glenn Norris <glenn@ohanagp.com>
Subject: PCI DSS 4 Compliance Training

By March 31, 2024, I need everyone to complete their assigned training. I understand this is short notice, and if you are unable to meet this deadline, please let me know when you can. After Mary 31, 2024, we may need to augment your responsibility if this is not completed.

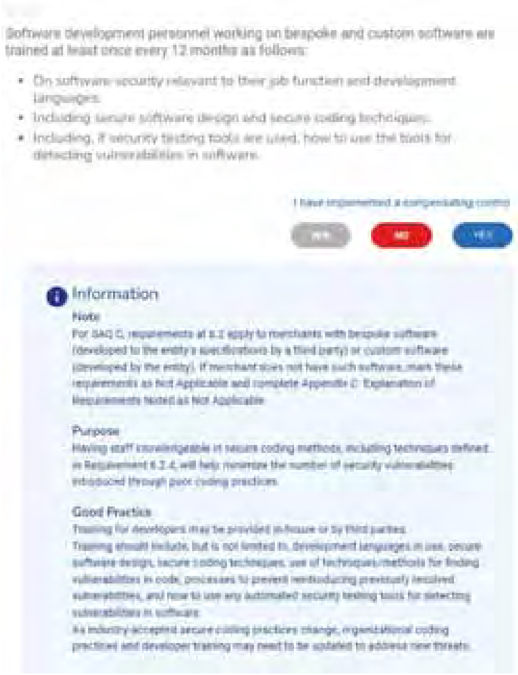
@Darren Koritzka @Dante Martinez @Rikki Francisco @Ann Pinera
Payment Card Industry (PCI) Data Security Standard (DSS) - Microsoft Compliance | Microsoft Learn
Review all the files in the PCI_DSS_QRG-v4.zip attachment

@Darren Koritzka @Dante Martinez @Ryan Brooks BC You also have
Best practices for the Microsoft identity platform - Microsoft identity platform | Microsoft Learn
Microsoft Entra ID and PCI-DSS Requirement 6 - Microsoft Entra | Microsoft Learn

@Ryan Brooks BC @Rikki Francisco @Ann Pinera You also have
Review all the files in the PCI-Secure-Software-Program

Do you need to remember 100% of this material, but here are some key takeaways:
@Ryan Brooks BC You have the highest level of PCI compliance requirement because you work onbespon bespokeoke software for us, and I need an exact date from you when you have completed this task because I am going to attest that you have affirmed to me compliance training   on that date. You need to understand the following concepts:

Exhibit 19N



Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows:

- On software security relevant to their job function and development languages.
- Including secure software design and secure coding techniques.
- Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.

I have implemented a compensating control

Information

Note

For SAQ C, requirements at 6.2 apply to merchants with bespoke software (developed to the entity's specifications by a third party) or custom software (developed by the entity). If merchant does not have such software, mark these requirements as Not Applicable and complete Appendix C: Explanation of Requirements Noted as Not Applicable.

Purpose

Having staff knowledgeable in secure coding methods, including techniques defined in Requirement 6.2.4, will help minimize the number of security vulnerabilities introduced through poor coding practices.

Good Practice

Training for developers may be provided in-house or by third parties.

Training should include, but is not limited to, development languages in use, secure software design, secure coding techniques, use of techniques/methods for finding vulnerabilities in code, processes to prevent reintroducing previously resolved vulnerabilities, and how to use any automated security testing tools for detecting vulnerabilities in software.

As industry-accepted secure coding practices change, organizational coding practices and developer training may need to be updated to address new threats.

I will need to "interview" you afterwards or you can provide the certification of a completed PCI DSS 4 software developer course. I will be using questions based on the PCI Compliance assessment that follows this question. You should be comfortable speaking about bugs, flaws, exploits, attacks and how to detect, prevent, test for, and remediate/resolve. You should understand concepts like CERTs and FIRST as a developer who has externally accessible applications inclusive of ones that are directly on a PCI compliant network and are used to input PCI data for transmission to a processor.

@Ryan Brooks BC @Darren Koritzka @Dante Martinez
You have a smaller scope of impact. Patch management, change control procedures, change control documentation and CERT and FIRST concepts. Focus on detection of exploits as they would impact your respective domains and become familiar with how we track zero day attacks and what we should do once they are made aware to us.

@Ann Pinera @Rikki Francisco @Ryan Brooks BC
You have the smallest scope which is focused on bugs that create vulnerabilities and you should understand the software life cycle, from stage to dev to production. Why they exist and what are we doing in those steps to detect and address potential attack vectors from our own code.

@Glenn Norris We should discuss where we feel this could be a need to address with OSI and Gross/Nectari. There is an physical assessment and remote assessment that we would have done by a qualified accessor, but I can tell you now that they will fail. Alternatively, we could require them to pass a certification course to demonstrate by 3rd party they have the required knowledge. Gross/Nectari I could argue never touch anything that could fall under the PCI scope, but that makes one small assumption that I need you/matt to attest to and that is we never in any way have our own credit card information recorded somewhere in any of those sage systems. Not the fragments on a receipt, but anything more should result in a conversation so we can determine our comfort level and we can review the standard as it applies. Most of this will be covered in section 6 if you want to review that or all of it, but please understand that I am attesting to this and I would like that conversation for my own peace of mind.

This message may include text created with the help of natural language processing.

Exhibit 19N

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

Exhibit 19O-1

From:	**Ryan Wagner**
Sent:	**Tuesday, May 21, 2024 9:03 PM**
To:	**Glenn Norris**
Cc:	**Justin Drummond; Rich Hartman; Karen Debus**
Subject:	**Re: REPEAT QUESTION - PCI DSS 4 Compliance Training**

Sorry, I misspoke in my last email. the Kiosk software is intended to facilitate the functionality mentioned below through another website. and do so while on the PCI compliant network.

Everything on that network needs to be PCI compliant. The Kiosk software needs to secure and we need to verify that it is. Since he wrote this software this absolutely qualifies. Since it is hosted on our azure system it then raises additional concerns.

I can not guarantee that this said in a way that can not be picked apart to find something wrong with it, but the general idea is accurate. Unfortunately you are asking me while I am unable to think at the same level I normally do.

Assuming you were able to think of something that did validate a scenario that we have no concerns, I am not sure that right now I could safely confirm your hypothesis. I really don't want to say yes – no problem.

You have made it clear that I need to do this and I am not sure if you have had a panic attack last for hours but it is exhausting and I don't want perform the work in this state which is why sometimes I can't work and need to take breaks then later on I can work on things.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093

www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 8:54 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>
Subject: Re: REPEAT QUESTION - PCI DSS 4 Compliance Training

Exhibit 19O-1

@Glenn Norris

I wish I could avoid checking my email right now, as it's not helping the situation. However, I want to address your concerns as clearly as possible.

First, I need to clarify that this is not a moot point. To make an informed decision, you need to ask the right questions, or the answers you get won’t be helpful.

One of the false assumptions here is that you are only aware of one of Ryan's solutions and assume this represents the entirety of his work.

Did you know that Ryan also developed the PFHQ-approved Kiosk platform? This platform is deployed on iPads at clubs, allowing users to input payment information directly into the PCI network. Furthermore, this solution is hosted in our Azure environment, which Ryan set up and deployed alone.

Given this information, it's crucial to determine if the AP Processing software developed by Baltimore Consulting has any PCI-compliant information that falls under PCI DSS 4 requirements. If no checking account or other sensitive payment information is involved, then the requirement may be less critical. However, we must thoroughly review all aspects to ensure compliance.

This is one example of where we need to first ask the right questions. In the state I am in, I don't think I can give a complete answer that encompasses every possible way that I have found or still need to look into, but it is something that needs to be done.

I am trying to comply with the mandate set forth, but we need to fully understand the scope of Ryan’s involvement and the potential risks to our compliance.

Thank you for your understanding.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

“Culture eats strategy for breakfast”

Exhibit 19O-1

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 7:42 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>
Subject: RE: REPEAT QUESTION - PCI DSS 4 Compliance Training

The question that I need answered is: Does the software package that Baltimore Consulting Developed for AP Processing have any PCI Compliant relative information that falls under the PCI DSS 4 requirements?

If the information in the AP Software application does not apply, then this requirement becomes mute.

No checking account information is in the software.

Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 6:27 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>
Subject: Re: REPEAT QUESTION - PCI DSS 4 Compliance Training

1. **Regarding Ryan Brooks:**

   - **Role**: Ryan is the only one creating custom software solutions for us.
   - **Attendance**: He is not attending meetings or participating in the process.
   - **Actions**: He is implementing changes without my knowledge that may not comply with the requirements.

When I assigned training to everyone, I told them that I would restrict their duties if necessary.

Geoff contacted me yesterday as a follow-up to an email from last week.

Exhibit 19O-1

As with the first bullet point, here is the requirement. This is not the same requirement that the other people on the team have because no one else is building custom software for us, but if they were then they would need to meet this same requirement.

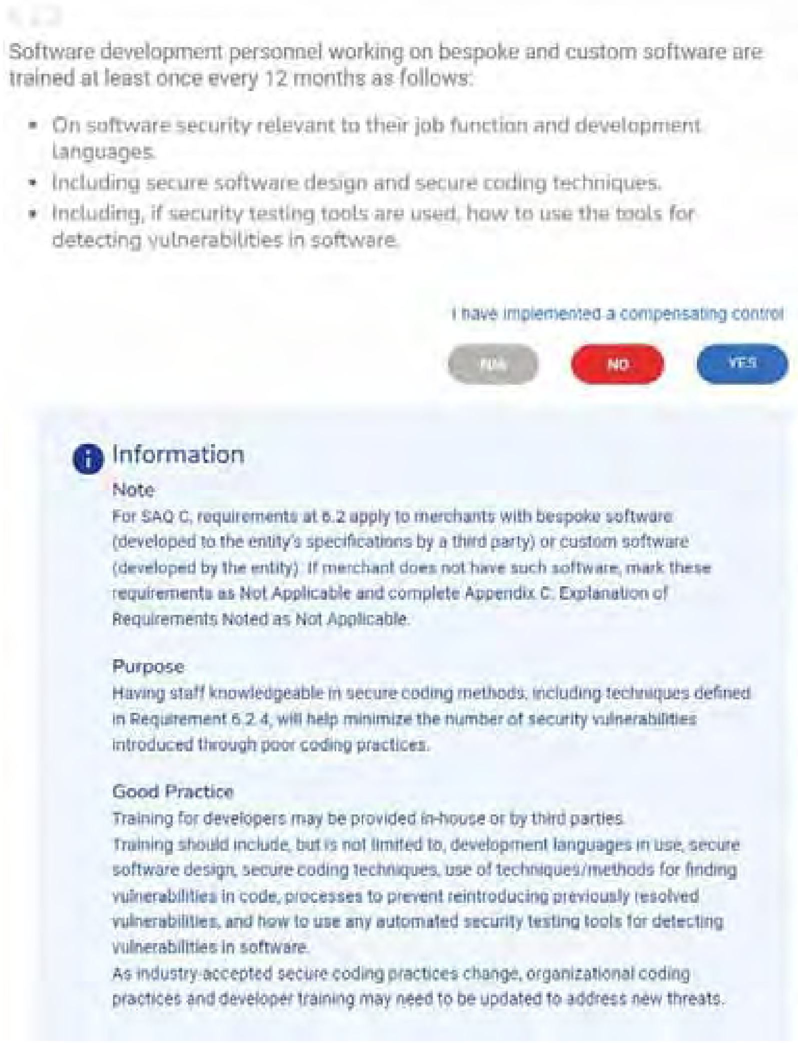
I find it odd that you constantly disagree and do not believe me, and my reply is --- let's go ask an expert. An investigator, a lawyer, and the head of corporate security. If I am wrong, then they would be the ones to tell us, and there would not be any issues. I do not understand why we don't do this on any of these topics; it has to be easier than this. You might not be in physical pain right now because of this and suffering from today, but I am and I don't deserve this. You never disagree with me – you disagree with the data, the math, the analytics, the experts, the manufacturers, and the company who wrote the OS and software, and all I ever do is show you what they said. What the data says. What the math says. What the analysis says. Or even just asking the question - why is this number so low? Why did we submit a number to the bank that was half what the invoices showed when we went through them one by one. Why did Rich immediately tell you and the 2 Cs that I filed an HR complaint about? Why are my role and responsibilities being stripped away? Why can't you let me do my job? when do I get to do my job?

Are you forcing me under duress to give Ryan Brooks access when the reason I could answer yes to this was because I removed him from the system and he can no longer make changes? I know that you said Yes do this or get written up.

I showed you what it said... you said you disagree --- with --- the PCI DSS 4 requirements? You don't disagree with me because I never said something to disagree with.

I don't deserve this... this is my opinion. I don't deserve to be treated like this. I don't deserve to be told that I use too many words and am too professional because I don't swear. I don't deserve to be made to feel like my greatest weakness is that I am not enough of "a man". well, I am not --- I am non-binary. I don't talk like you because I am not like you. I do however believe that I embody everything this company says they stand for, and for months I have tried to convince you to listen to an expert before your actions are seen in a manner that causes you to end up in an orange jump suit. The more I try to prevent you from making decisions with the potential for serious consequences you attack and attack and attack. I don't deserve this... those are my opinions and you are free to disagree

Exhibit 19O-1



6.2.2

Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows:

- On software security relevant to their job function and development languages.
- Including secure software design and secure coding techniques.
- Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.

I have implemented a compensating control

Information

Note

For SAQ C, requirements at 6.2 apply to merchants with bespoke software (developed to the entity's specifications by a third party) or custom software (developed by the entity). If merchant does not have such software, mark these requirements as Not Applicable and complete Appendix C: Explanation of Requirements Noted as Not Applicable.

Purpose

Having staff knowledgeable in secure coding methods, including techniques defined in Requirement 6.2.4, will help minimize the number of security vulnerabilities introduced through poor coding practices.

Good Practice

Training for developers may be provided in-house or by third parties.

Training should include, but is not limited to, development languages in use, secure software design, secure coding techniques, use of techniques/methods for finding vulnerabilities in code, processes to prevent reintroducing previously resolved vulnerabilities, and how to use any automated security testing tools for detecting vulnerabilities in software.

As industry-accepted secure coding practices change, organizational coding practices and developer training may need to be updated to address new threats.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 5:59 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus

Exhibit 19O-1

<karen.debus@ohanagp.com>; Glenn Norris <glenn@ohanagp.com>
Subject: REPEAT QUESTION - PCI DSS 4 Compliance Training

Ryan, I asked you this question yesterday with no response. Please answer this question. Did everyone listed below take their course except Ryan Brooks?

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Monday, May 20, 2024 3:05 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>
Subject: Re: PCI DSS 4 Compliance Training

Yes - Geoff is the head of IT security at PFHQ. This set of questions applies to Ryan Brooks for the work he does for us with our custom software solutions.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Monday, May 20, 2024 2:06 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>
Subject: RE: PCI DSS 4 Compliance Training

Exhibit 19O-1

Ryan, is Geoff from Corp? If so, are they requiring us to complete PCI Standards on line? Did everyone listed below take their course except Ryan Brooks?

Let’s discuss.

Thank you, Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

OHANA
Growth Partners

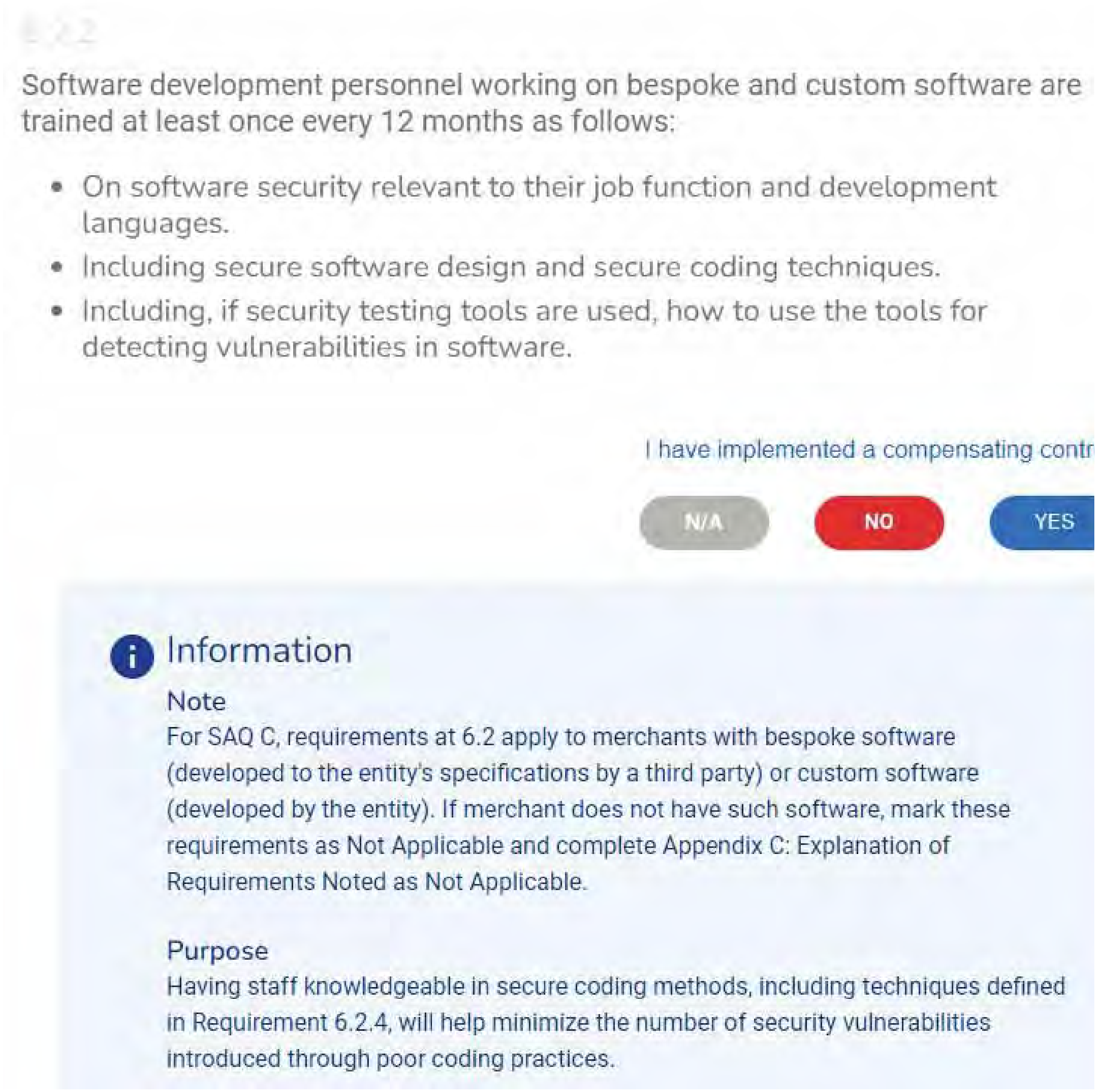
office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

“Culture eats strategy for breakfast”

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Monday, May 20, 2024 1:34 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>
Subject: Re: PCI DSS 4 Compliance Training

@Glenn Norris I got Geoff asking if we can wrap up our assessment for DSS4. We are still stuck on the training requirement for RB because he doesn't have time to complete the required PCI training. What would you like to do about this?

Exhibit 19O-1



6.2.2

Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows:

- On software security relevant to their job function and development languages.
- Including secure software design and secure coding techniques.
- Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.

I have implemented a compensating contr

Information

Note

For SAQ C, requirements at 6.2 apply to merchants with bespoke software (developed to the entity's specifications by a third party) or custom software (developed by the entity). If merchant does not have such software, mark these requirements as Not Applicable and complete Appendix C: Explanation of Requirements Noted as Not Applicable.

Purpose

Having staff knowledgeable in secure coding methods, including techniques defined in Requirement 6.2.4, will help minimize the number of security vulnerabilities introduced through poor coding practices.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

Exhibit 19O-1

OHANA
Growth Partners

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Thursday, March 21, 2024 5:03 PM
To: Ryan Brooks BC <rb@baltimoreconsulting.com>; Darren Koritzka <Darren.Koritzka@ohanagp.com>; Dante Martinez <dante.martinez@ohanagp.com>; Rikki Francisco <rikki.francisco@ohanagp.com>; Ann Pinera <Mareann.Pinera@ohanagp.com>; Glenn Norris <glenn@ohanagp.com>
Subject: PCI DSS 4 Compliance Training

By March 31, 2024, I need everyone to complete their assigned training. I understand this is short notice, and if you are unable to meet this deadline, please let me know when you can. After Mary 31, 2024, we may need to augment your responsibility if this is not completed.

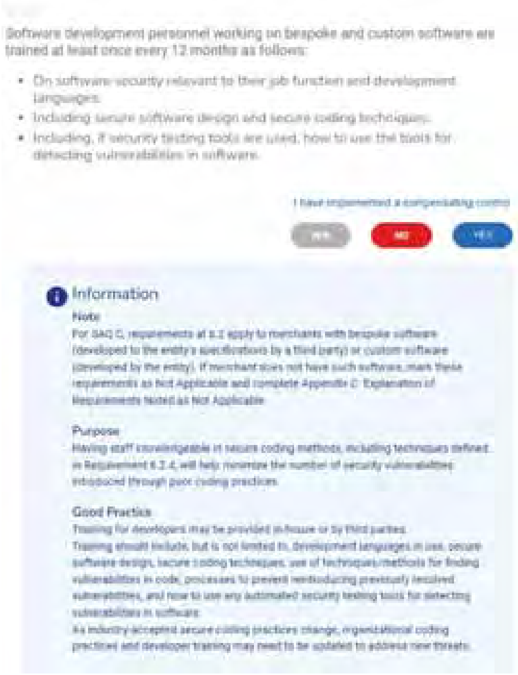
@Darren Koritzka @Dante Martinez @Rikki Francisco @Ann Pinera
Payment Card Industry (PCI) Data Security Standard (DSS) - Microsoft Compliance | Microsoft Learn
Review all the files in the PCI_DSS_QRG-v4.zip attachment

@Darren Koritzka @Dante Martinez @Ryan Brooks BC You also have
Best practices for the Microsoft identity platform - Microsoft identity platform | Microsoft Learn
Microsoft Entra ID and PCI-DSS Requirement 6 - Microsoft Entra | Microsoft Learn

@Ryan Brooks BC @Rikki Francisco @Ann Pinera You also have
Review all the files in the PCI-Secure-Software-Program

Do you need to remember 100% of this material, but here are some key takeaways:
@Ryan Brooks BC You have the highest level of PCI compliance requirement because you work onbespon bespokeoke software for us, and I need an exact date from you when you have completed this task because I am going to attest that you have affirmed to me compliance training on that date. You need to understand the following concepts:

Exhibit 19O-1



Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows:

- On software security relevant to their job function and development languages.
- Including secure software design and secure coding techniques.
- Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.

I have implemented a compensating control

Information

Note

For SAQ C, requirements at 6.2 apply to merchants with bespoke software (developed to the entity's specifications by a third party) or custom software (developed by the entity). If merchant does not have such software, mark these requirements as Not Applicable and complete Appendix C: Explanation of Requirements Noted as Not Applicable.

Purpose

Having staff knowledgeable in secure coding methods, including techniques defined in Requirement 6.2.4, will help minimize the number of security vulnerabilities introduced through poor coding practices.

Good Practice

Training for developers may be provided in-house or by third parties.

Training should include, but is not limited to, development languages in use, secure software design, secure coding techniques, use of techniques/methods for finding vulnerabilities in code, processes to prevent reintroducing previously resolved vulnerabilities, and how to use any automated security testing tools for detecting vulnerabilities in software.

As industry-accepted secure coding practices change, organizational coding practices and developer training may need to be updated to address new threats.

I will need to "interview" you afterwards or you can provide the certification of a completed PCI DSS 4 software developer course. I will be using questions based on the PCI Compliance assessment that follows this question. You should be comfortable speaking about bugs, flaws, exploits, attacks and how to detect, prevent, test for, and remediate/resolve. You should understand concepts like CERTs and FIRST as a developer who has externally accessible applications inclusive of ones that are directly on a PCI compliant network and are used to input PCI data for transmission to a processor.

@Ryan Brooks BC @Darren Koritzka @Dante Martinez
You have a smaller scope of impact. Patch management, change control procedures, change control documentation and CERT and FIRST concepts. Focus on detection of exploits as they would impact your respective domains and become familiar with how we track zero day attacks and what we should do once they are made aware to us.

@Ann Pinera @Rikki Francisco @Ryan Brooks BC
You have the smallest scope which is focused on bugs that create vulnerabilities and you should understand the software life cycle, from stage to dev to production. Why they exist and what are we doing in those steps to detect and address potential attack vectors from our own code.

@Glenn Norris We should discuss where we feel this could be a need to address with OSI and Gross/Nectari. There is an physical assessment and remote assessment that we would have done by a qualified accessor, but I can tell you now that they will fail. Alternatively, we could require them to pass a certification course to demonstrate by 3rd party they have the required knowledge. Gross/Nectari I could argue never touch anything that could fall under the PCI scope, but that makes one small assumption that I need you/matt to attest to and that is we never in any way have our own credit card information recorded somewhere in any of those sage systems. Not the fragments on a receipt, but anything more should result in a conversation so we can determine our comfort level and we can review the standard as it applies. Most of this will be covered in section 6 if you want to review that or all of it, but please understand that I am attesting to this and I would like that conversation for my own peace of mind.

This message may include text created with the help of natural language processing.

Exhibit 19O-1

[Book time to meet with me](#)

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
[www.planetfitness.com](#)

"Culture eats strategy for breakfast"

Exhibit 19O-2

From:	**Ryan Wagner**
Sent:	**Tuesday, May 21, 2024 5:37 PM**
To:	**Glenn Norris**
Cc:	**Justin Drummond; Rich Hartman; Karen Debus; Matt Norris**
Subject:	**Re: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS**

Thank you for your response. I will send Ryan Brooks the link to complete the PCI DSS 4.0 training and ensure he begins the required processes immediately. However, I must reiterate that reinstating his access without him having completed these steps will place us in violation of PCI DSS 4.0 compliance requirements.

Immediate Actions:

1. Ryan Brooks can choose any available training program as long as we receive proof of completion. Previously, I offered to sit down with him to ensure he understands the necessary information, but under duress, I am not comfortable doing this because of the ongoing threats and pressure, which I am afraid will continue until I certify him regardless of his actual compliance.

2. Restore Access Under Duress: I will reinstate his access as per your directive. This action is being taken under duress and against my professional judgment due to the compliance risks involved.

I must inform you that I am experiencing severe stress and anxiety due to this situation, including a panic attack and hyperventilation throughout this conversation. I am currently shaking badly and struggling to finish this email. If I am unable to complete this task by 9 am tomorrow, it is because I have gone catatonic from this experience. Please understand that I am doing my best under these circumstances.

I strongly advise documenting this decision and the associated risks to protect the company and ourselves. I have also reached out to Geoff VanMaastricht to seek his assistance in finding a long-term solution that ensures compliance.

Thank you for your understanding.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

Exhibit 19O-2

OHANA
Growth Partners

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093

www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 5:28 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: RE: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

Send Ryan Brooks the Link to complete the PCI DSS 4.0 training and processes. I still want his access returned immediately.

Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 5:13 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: Re: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

I acknowledge your directive and understand the urgency of the situation. However, I must reiterate the compliance risks associated with reinstating Ryan Brooks' access without him completing the necessary PCI DSS 4.0 training and processes.

As the head of IT, my primary responsibility is to ensure that we maintain compliance with all regulatory standards. Restoring Ryan's access without meeting these requirements places our PCI DSS 4.0 certification and the company at significant risk. While I am prepared to follow your instructions, I must stress that this action is being undertaken under duress due to your explicit directive.

Exhibit 19O-2

I have reached out to Geoff VanMaastricht, our head of corporate security, to seek his assistance in finding a solution that balances our compliance obligations with your request. Here is the email I sent to him, which includes you and President Justin Drummond in the loop:

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner Ryan.Wagner@ohanagp.com
Sent: Tuesday, May 21, 2024 5:09 PM
To: Geoff VanMaastricht Geoff.VanMaastricht@pfhq.com
Cc: Glenn Norris glenn@ohanagp.com; Justin Drummond Justin.Drummond@ohanagp.com
Subject: SAQ - PCI Compliance: We need your assistance

@Geoff VanMaastricht, Would you be available for a meeting tomorrow to discuss this and related PCI Compliance concerns? I am being told to reinstate the same person, but they refuse to do the training, take part in the code review, change control, or any other process to maintain compliance. I don't know what to do and could use your assistance to find a solution that works for our CFO as well as meet the compliance requirements.

To mitigate these risks and protect our compliance standing, I propose the following steps:

Immediate Compliance Training: Expedite Ryan's PCI DSS 4.0 compliance training and ensure it is completed as a top priority.
Temporary Limited Access: Provide Ryan with limited access necessary for immediate tasks, under close monitoring, until he completes the required training and processes.
Documented Agreement: Document this course of action, including the acknowledgment that this decision is made under duress, to protect both the company and ourselves, ensuring we have a record of our compliance efforts and the rationale behind these decisions.
I am available to discuss this further and facilitate any immediate actions required to address your concerns while maintaining our compliance obligations.

Please let me know how you would like to proceed.

Best regards,

This message may include text created with the help of natural language processing.

Book time to meet with me

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 5:05 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>

Exhibit 19O-2

Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: RE: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

Rich, please prepare a write up for me .

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 5:02 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: Re: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

@Glenn Norris

Thank you for your prompt response. I understand the urgency of your request, but I must reiterate the compliance requirements and potential risks involved in reinstating Ryan Brooks' access without completing the necessary PCI DSS 4.0 training and processes.

Reinstating his access without compliance would put our certification at risk and could have serious legal and security implications for the company. As the head of IT, I have a responsibility to ensure that we adhere to these standards.

Given the gravity of the situation and your directive, I propose a meeting tomorrow morning with you, myself, and the head of corporate security to discuss how we can address this matter without compromising our compliance obligations. This will allow us to find a solution that meets your needs while safeguarding our compliance and security standards.

Please confirm a suitable time for this meeting.

Thank you for your understanding.

This message may include text created with the help of natural language processing.

Book time to meet with me

Exhibit 19O-2

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 4:59 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: RE: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

If Ryan Brooks does not have access by tomorrow morning , you will be written up for insubordination. Is that clear? Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 4:56 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: Re: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

Thank you for your email. I understand your concerns and would like to clarify the situation regarding Ryan Brooks' access and our compliance requirements.

Compliance and Access Issues:

Exhibit 19O-2

Yesterday, I consulted with PFHQ about how to handle situations where personnel had not completed required training. Before I could act on the conversation, Ryan Brooks informed me he didn't have time for a mandatory 15-minute meeting, and he had already stated he couldn't complete the required training or other tasks assigned to him. Consequently, I removed him to resolve the block to completing the SAQ, as instructed by PFHQ.

Overnight Changes:

The compliance issues did not change overnight. What changed was the final decision to remove Ryan after he explicitly refused to engage in critical compliance activities. Reinstating his access today would violate PCI DSS 4.0 standards, as I have already informed the head of corporate security that the compliance issue was resolved by terminating his access.

Performance Concerns:

The issues identified by Matt, as well as numerous concerns raised by the accounting department, reflect the quality of Ryan's work. While being responsive is important, it is more critical to ensure that work aligns with our strategic objectives and compliance requirements and does not result in these problems existing. Since September/October, Ryan's recommendations have moved us further from resolution, as evidenced by the ongoing issues highlighted in Matt's email.

Ryan's inability to complete tasks assigned to him and his mismanagement of resources (e.g., setting up a second AVD environment, doubling costs, ignoring Microsoft's recommendations) demonstrate a lack of alignment with our strategic direction. His actions, including making unauthorized changes, have exacerbated our challenges rather than resolving them.

Historical Context:

From the start of the emergency migration project, Ryan proposed outdated solutions, like reinvesting in an old AC system instead of modernizing our platform. Following my HR complaint in November, you stopped supporting the initial proposal and allowed Ryan to make changes against our needs, often in secret. Before my FMLA leave, you reinstated his access despite my concerns. Since FMLA, you and Ryan have been in charge of the IT department. Recently, you informed me I should no longer step back, allowing me to re-establish control and initiate daily standups and other processes to get the team back on track.

Next Steps:

Given the situation:

Ryan must complete the PCI DSS compliance training and participate in the required processes before his access can be reinstated.
Restoring his access without meeting these requirements would jeopardize our PCI DSS 4.0 compliance.
I am committed to resolving these issues in a manner that upholds our compliance standards and addresses our operational needs. Please review the data, recommendations, and conclusions from Microsoft and our current state of issues, which collectively indicate that Ryan is not currently qualified to manage our cloud environment.

We can review these concerns with the head of corporate security, and if I understand why it must happen today, perhaps I can offer a solution that does not result in PCI compliance issues.

Thank you for your understanding and cooperation.

This message may include text created with the help of natural language processing.

Exhibit 19O-2

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 4:28 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: RE: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

How was Ryan Brooks allowed access yesterday and not today? What changed overnight, it does not make sense that compliance issues were just discovered and changed overnight.

I do not think your stance flies.

Please do as I have instructed you. He will take the test.

See Matt's reason why we need him. Look at attached email.

Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 3:38 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: Re: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

Exhibit 19O-2

@Glenn Norris

Thank you for your email. I understand your urgency regarding Ryan Brooks' access and want to ensure we handle this appropriately while maintaining our compliance with PCI DSS 4.0 standards.

1. Mandates and Requirements:
   - PFHQ mandates compliance with PCI DSS 4.0, which outlines the specific requirements for all personnel with access to sensitive data and systems. This includes mandatory training and participation in key security processes.
2. Attestation Filings:
   - PFHQ instructed me to complete the attestation filings, which are necessary to certify our compliance with PCI DSS 4.0. These filings were submitted to our compliance auditors and relevant regulatory bodies to confirm that we meet all required security standards.
3. Ryan Brooks' Access:
   - Restoring Ryan Brooks' access without him completing the required training and participating in mandated security processes would violate our PCI DSS 4.0 compliance. This could jeopardize our certification and the security of our systems.

Could you please clarify the consequences you foresee if we do not restore Ryan's access today? Understanding your concerns will help us address them while ensuring we remain compliant with PCI DSS 4.0 standards.

I must emphasize that compliance with these standards is critical to our operations and security. I am committed to resolving this situation as quickly as possible within the bounds of our compliance requirements.

Please let me know how you would like to proceed, and we can work together to find a solution that maintains our compliance and addresses your needs.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

Exhibit 19O-2

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 3:26 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: RE: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

1. Please explain who is mandating this and what it entails.
2. Stop filing attestation filings- who gets these and why were they sent in the last 24 hours?
3. I WANT RYAN'S ACCESS RESTORED TODAY. CONFIRM WHEN THIS IS COMPLETED

Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 2:08 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>
Subject: Re: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

@Glenn Norris I hope this message finds you well. I appreciate your prompt response regarding Ryan Brooks' compliance and performance. I would like to address the points you raised to ensure clarity and alignment with our compliance requirements and performance expectations.

Compliance Allegations:
Regarding the compliance allegations, it is crucial to clarify that all team members, including vendors, must complete the required PCI DSS compliance training. This is a non-negotiable requirement to maintain our certification and ensure our systems' security and integrity. If Ryan was previously informed that he did not need to complete this training, that was incorrect, and I appreciate his willingness to rectify this.

Compliance Training Requirement:
Ryan must complete the PCI DSS compliance training before he can resume any work, as our attestation has already been filed.
Additional Compliance Requirements:

Beyond the training, Ryan's access has been restricted due to his lack of participation in several PCI DSS-required processes. These include:

Exhibit 19O-2

Participation in daily standup meetings
Involvement in the change control review board
Engagement in the pipeline for code publishing
Adherence to other necessary procedures
Ryan has previously refused to engage in these processes, which are critical for maintaining our compliance. Additionally, the partial work he has completed has not met PCI DSS compliance standards, and I have had to redo this work to align with our requirements.

Access and Admin Rights:
Regarding your directive to restore Ryan's admin rights immediately, I must emphasize that any such action must comply with our PCI DSS 4 standards. Until Ryan completes the required compliance steps and demonstrates his understanding of PCI DSS requirements, he will not be able to make changes to any system as an administrator. This includes both his software engineer responsibilities and sufficient training for administration.

Next Steps:

Ryan must complete the PCI DSS compliance training immediately.HE IS DOING THIS
Ryan must participate in all PCI DSS required processes, including daily standups, change control review boards, and code publishing pipelines. I DO NOT AGREE
After Ryan completes the training and engages in these processes, we need detailed information on the specific tasks you want him to perform. This will allow us to assign him the least privileged access necessary to maintain PCI compliance.

If you feel it would be helpful, I am open to arranging a meeting with the corporate head of security to weigh in on these items and provide additional perspective on maintaining our compliance and security standards. NO THANK YOU

Thank you for your understanding and cooperation in ensuring we maintain our compliance and security standards. I look forward to resolving this matter collaboratively. I DO NOT AGREE WITH YOUR POSITIONS

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

Exhibit 19O-2

From: Glenn Norris <glenn@ohanagp.com>
Sent: Tuesday, May 21, 2024 1:48 PM
To: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>; Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Matt Norris <Matt.Norris@ohanagp.com>; Glenn Norris <glenn@ohanagp.com>
Subject: Ryan Brooks - REPLY TO YOU ALLEGATIONS & PERFORMANCE ISSUES OF RYAN BROOKS

Ryan, I do not agree with your performance and compliance allegations of Ryan Brooks. I asked him if he was required by you to complete the compliance PCI tests and he was adamant that you stated months ago that he did not need to complete this. He is willing to do it. This is straight from Ryan Brooks.

Regarding his performance, we need to have a conversation on your expectations and role for BC/RB. In my opinion, he has been and still is a valued vendor for our IT needs .

Please ask Justin, Rich, Matt or Karen(and others) how they do or do not value his contribution to our IT needs.

As I stated in our call earlier today, I want his admin rights restored today. There was no discussion with me about this action – I do not approve.

SEE COMMENTS IN RED BELOW

Thank you, Glenn

Glenn Norris
Chief Financial Officer
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x108
cell 410-365-2591
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 21, 2024 1:16 PM
To: Glenn Norris <glenn@ohanagp.com>
Cc: Justin Drummond <Justin.Drummond@ohanagp.com>
Subject: Ryan Brooks - More Info Needed

@Glenn Norris, I hope you're doing well. I am seeking clarification regarding your directive to retain Ryan Brooks in the IT Department. When we talked today, you expressed a specific need for his services, despite my concerns about his performance and our compliance requirements.

In addition, As part of our compliance with PCI DSS 4 standards, which I recently certified after significant efforts, every team member must meet the requirements. Ryan Brooks' refusal to follow proper procedures and complete

Exhibit 19O-2

the required upskill training posed a substantial obstacle to maintaining PCI DSS 4 unless he is able to do the things that I have required of him.

To clarify:

1. Security Training: Ryan has not completed the mandatory security training, which disqualifies him from being employed as a software engineer under PCI DSS 4 standards. HE WILL DO THIS IF IT IS REQUIRED.

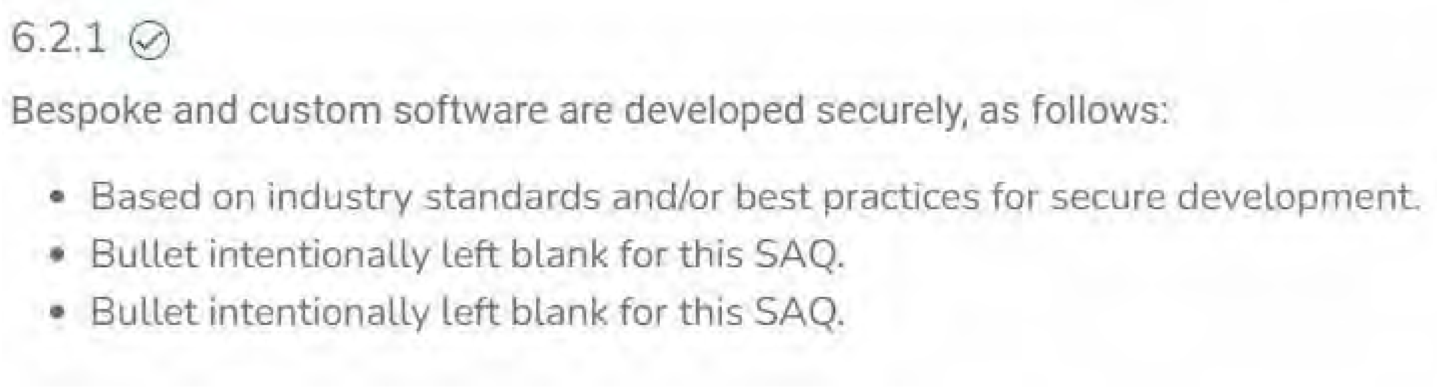
2. Code Review Process: He has been unable to participate in the code review process, making him unsuitable for automation or SQL work. WHAT IS THE REQUIRED TIME INVESTMENT HERE?

3. Change Control Review Board: Ryan's lack of participation in the change control review board precludes him from performing any sysadmin tasks or handling M365 or Azure responsibilities. HE HAS BEEN ON EVERY TUESDAY 230 CALL AND YOU GHOSTED THAT CALL ON 5-7-24 AND HE WAS IN ATTENDANCE. HE WILL NOT BE ON TODAY’S CALL SINCE YOU INADVERTANTLY FIRED HIM YESTERDAY.

Given these compliance issues, retaining Ryan to work in these areas conflicts with the PCI DSS 4 standards. His non-compliance and refusal to adhere to required protocols undermine our efforts to maintain these critical standards.

Please provide specific details regarding the necessity of retaining Ryan's services and ensure that it does not conflict with our PCI DSS 4 compliance requirements. I would like you to know that understanding your rationale and how it aligns with these standards is essential for moving forward.

Thank you for your attention to this matter. I look forward to your response to resolve this issue in compliance with our obligations.

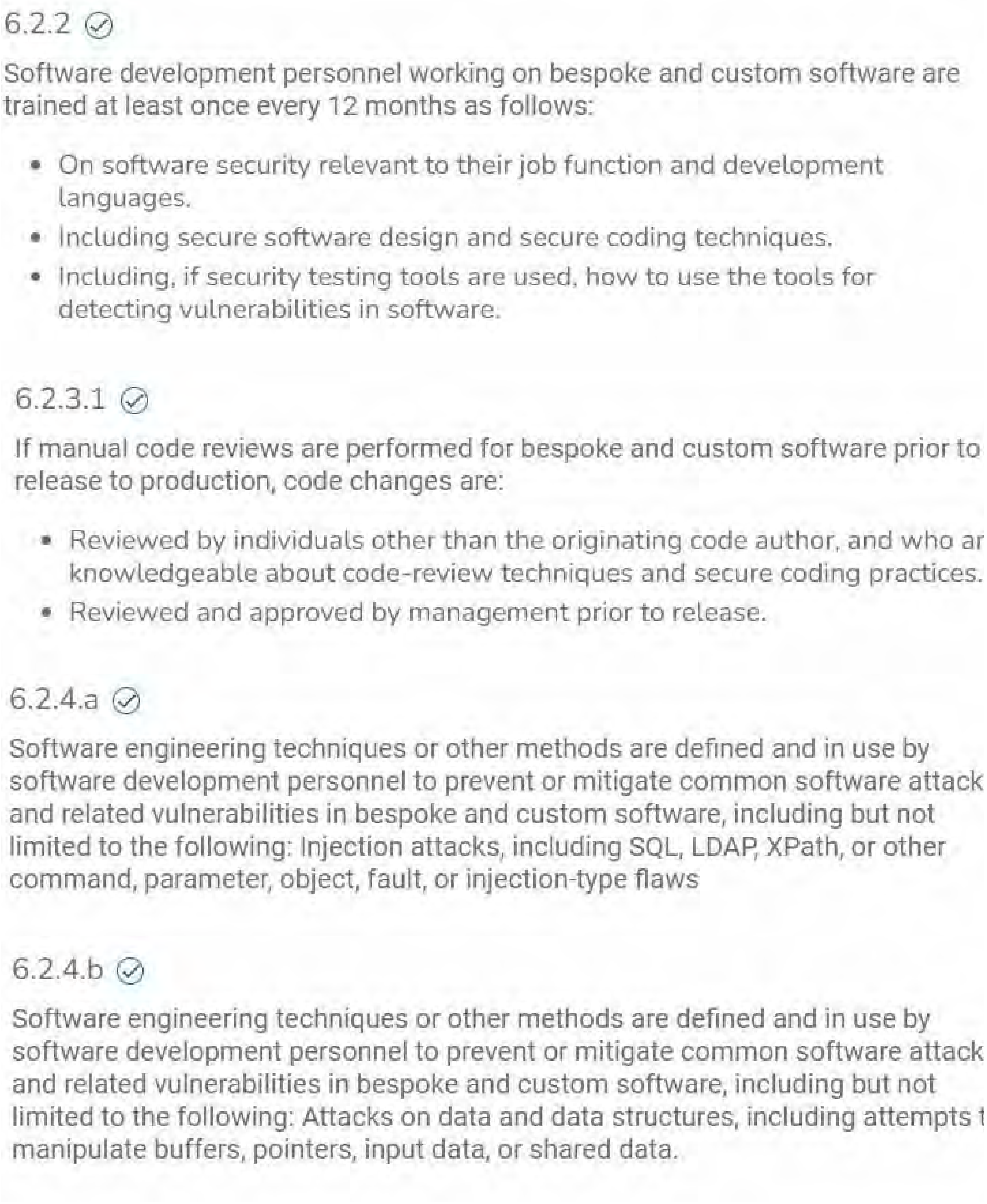


6.2.1 ✓

Bespoke and custom software are developed securely, as follows:

- Based on industry standards and/or best practices for secure development.
- Bullet intentionally left blank for this SAQ.
- Bullet intentionally left blank for this SAQ.

Exhibit 19O-2



6.2.2 ✓

Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows:

- On software security relevant to their job function and development languages.
- Including secure software design and secure coding techniques.
- Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.

6.2.3.1 ✓

If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are:

- Reviewed by individuals other than the originating code author, and who ar knowledgeable about code-review techniques and secure coding practices.
- Reviewed and approved by management prior to release.

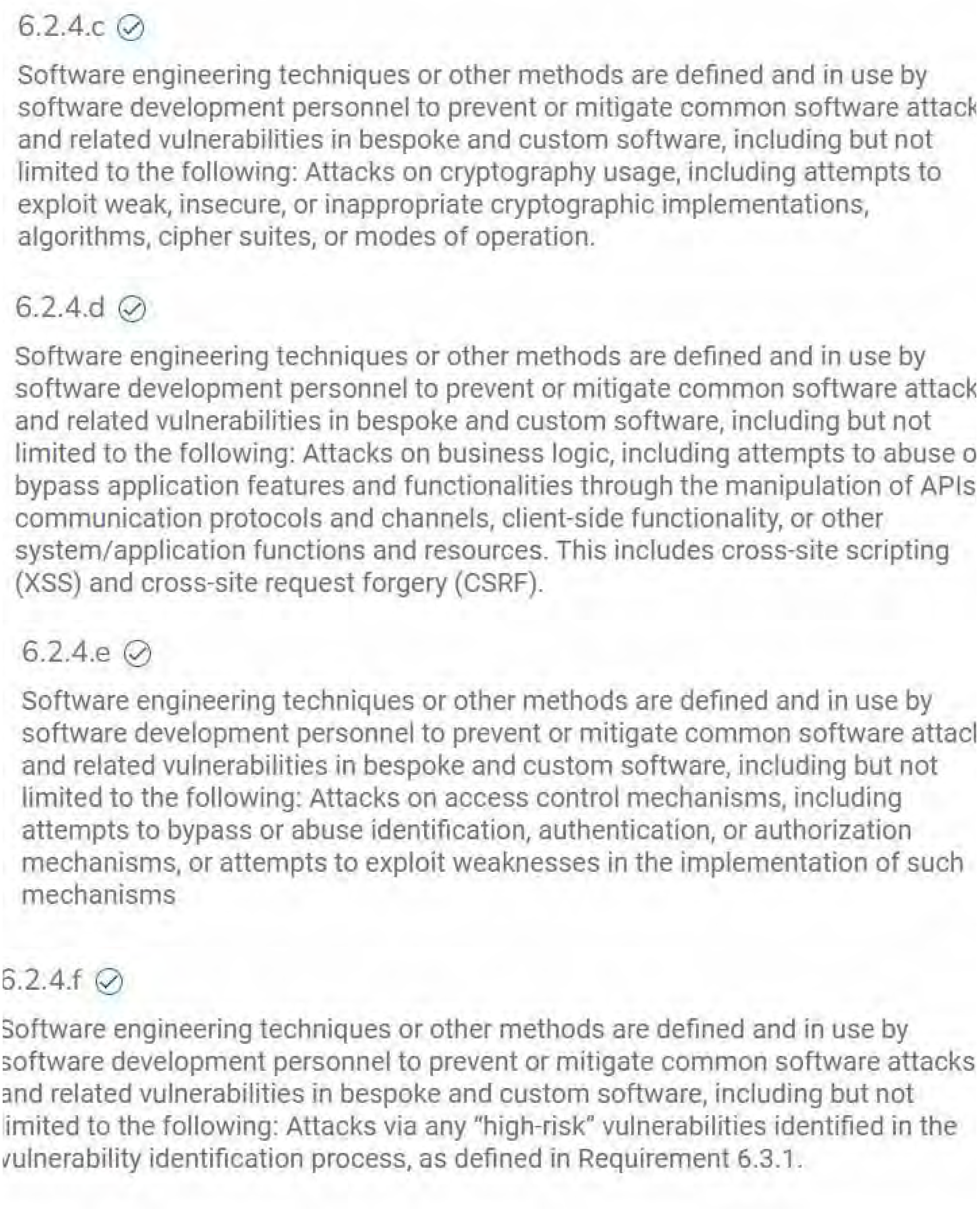
6.2.4.a ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws

6.2.4.b ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on data and data structures, including attempts t manipulate buffers, pointers, input data, or shared data.

Exhibit 19O-2



6.2.4.c ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation.

6.2.4.d ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attack and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on business logic, including attempts to abuse o bypass application features and functionalities through the manipulation of APIs communication protocols and channels, client-side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF).

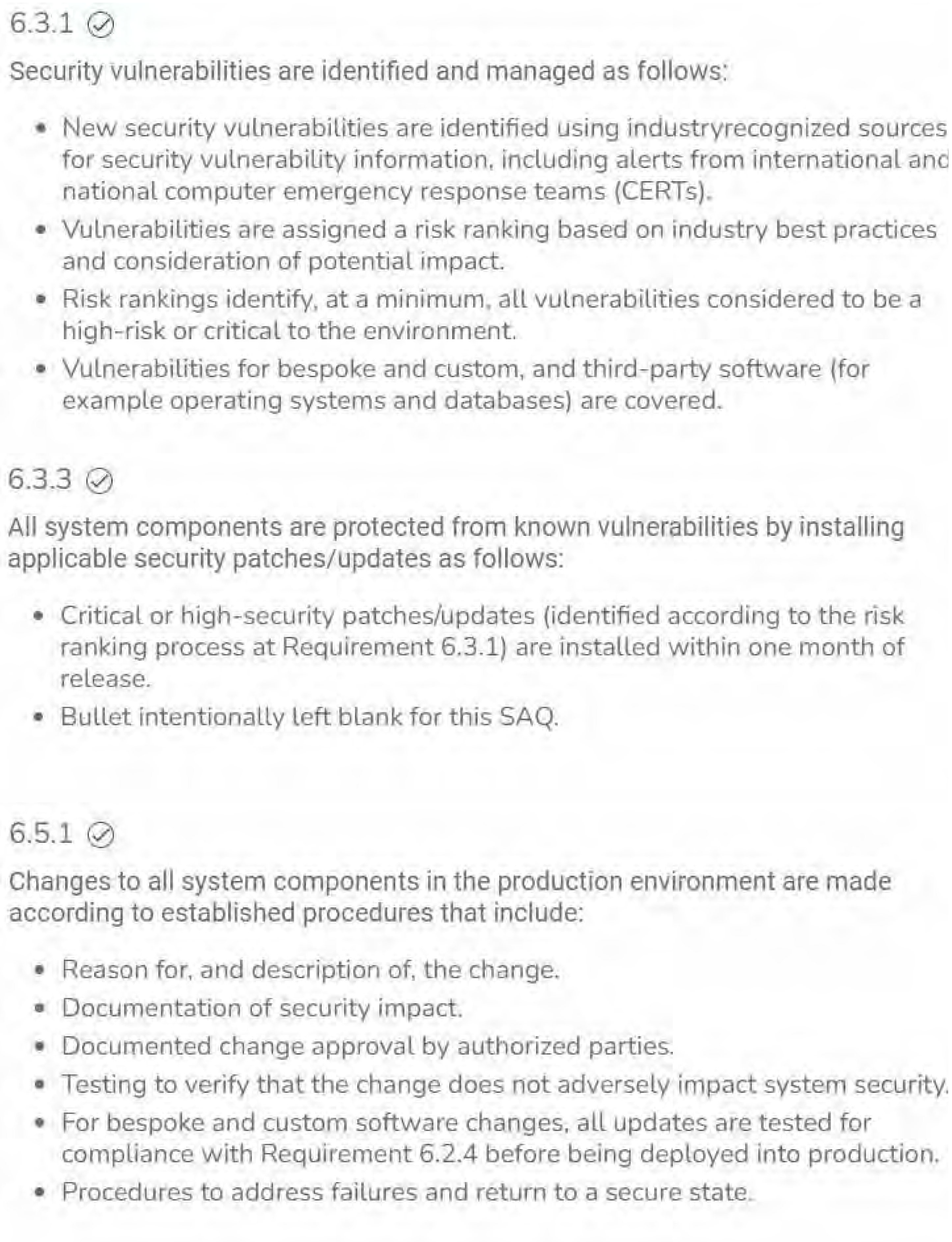
6.2.4.e ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacl and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms

6.2.4.f ✓

Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following: Attacks via any “high-risk” vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1.

Exhibit 19O-2



6.3.1 ✓

Security vulnerabilities are identified and managed as follows:

- New security vulnerabilities are identified using industryrecognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).
- Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.
- Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.
- Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.

6.3.3 ✓

All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows:

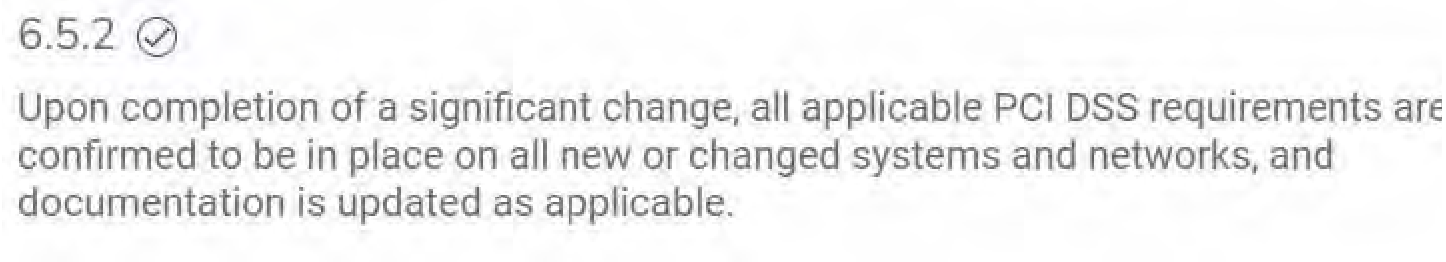
- Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release.
- Bullet intentionally left blank for this SAQ.

6.5.1 ✓

Changes to all system components in the production environment are made according to established procedures that include:

- Reason for, and description of, the change.
- Documentation of security impact.
- Documented change approval by authorized parties.
- Testing to verify that the change does not adversely impact system security.
- For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production.
- Procedures to address failures and return to a secure state.

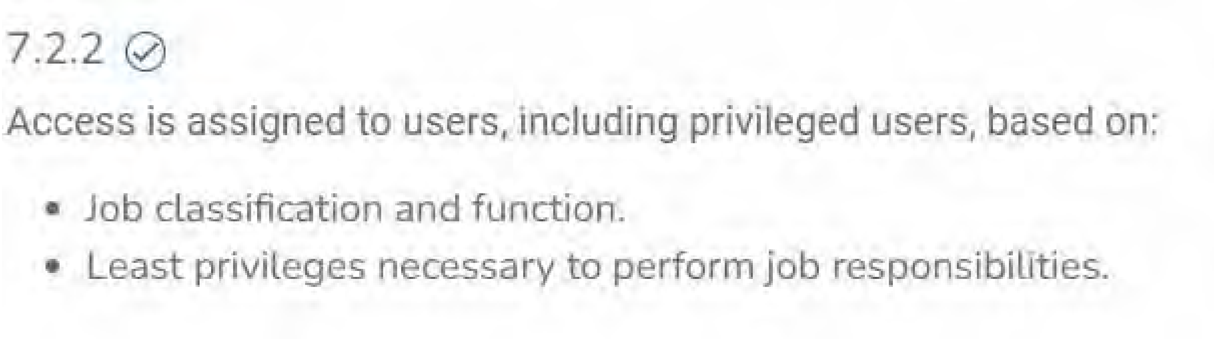
Exhibit 19O-2



6.5.2 ✓

Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.

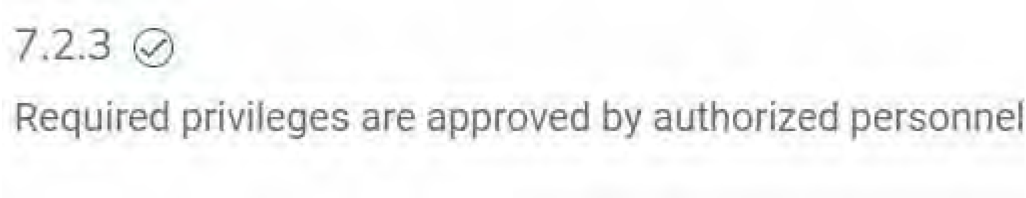
Please provide specific details regarding the necessity of retaining Ryan's services which does not conflict with our PCI DSS 4 compliance requirements. I would like you to know that understanding your rationale and how it aligns with these standards is essential for moving forward by assigning him permissions that will give him the least privileges necessary while not performing tasks listed above or otherwise in the PCI DSS 4.



7.2.2 ✓

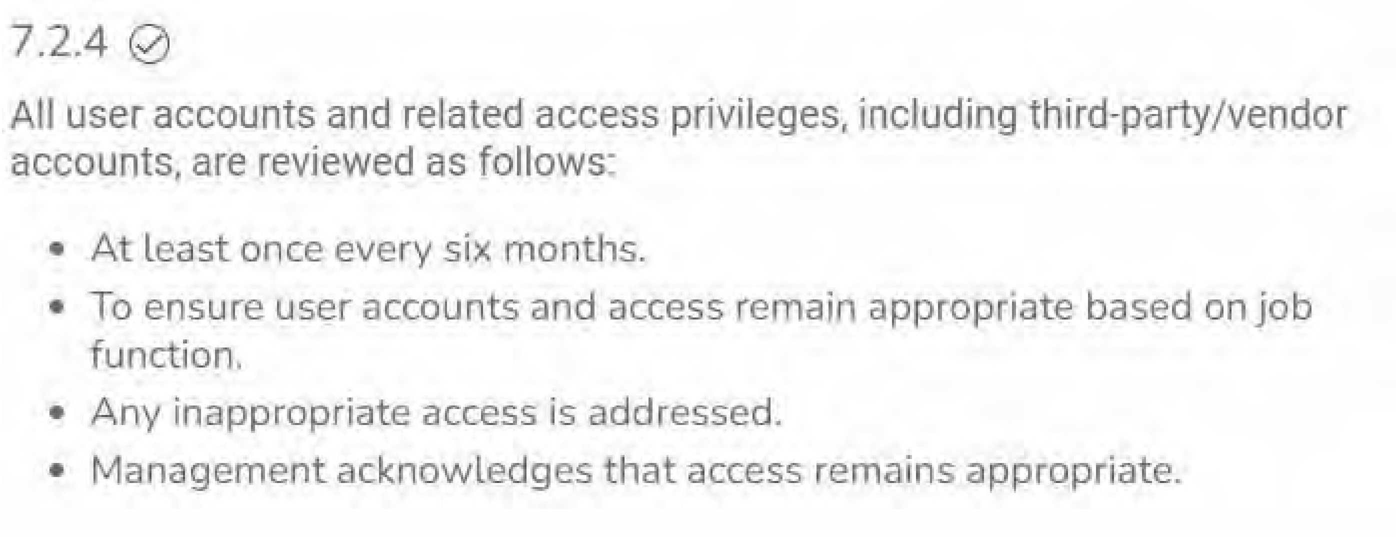
Access is assigned to users, including privileged users, based on:

- Job classification and function.
- Least privileges necessary to perform job responsibilities.



7.2.3 ✓

Required privileges are approved by authorized personnel



7.2.4 ✓

All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows:

- At least once every six months.
- To ensure user accounts and access remain appropriate based on job function.
- Any inappropriate access is addressed.
- Management acknowledges that access remains appropriate.

Thank you for your attention to this matter. I look forward to your response and to resolving this issue in accordance with our obligations.

Exhibit 19O-2

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

"Culture eats strategy for breakfast"

Exhibit 24E-2

rdc

From: Ryan Wagner
Sent: Wednesday, May 29, 2024 3:05 PM
To: Glenn Norris; Justin Drummond; Stacey Wittelsberger (ESC); C. Victor Brick; Lynne Brick B.S.N. M.A.; Terry Woods (Planet Fitness); Earl Ihle
Cc: Rich Hartman; Karen Debus
Subject: Re: Finchloom Flight Program

As you may recall, on May 8th, I raised concerns regarding Ryan Brooks' insubordination, evidenced by his refusal to attend required meetings, disregard for procedures, and failure to complete any tasks assigned this year. In response, Glenn instructed me to "get it done," reversing a prior directive from January, which reduced my job function and resulted in Glenn directly managing the IT Department since my FMLA leave.

Here are notable examples from this year (this list is not exhaustive):

1. SQL Developer Acquisition: When I thanked Glenn for adopting my recommendation to hire a new SQL developer, I asked why I was excluded from the vetting process. Glenn informed me that my input was not needed.

2. Meeting Exclusion: I was instructed to stop attending weekly Comcast meetings. When I offered to assist Glenn with the Comcast Credits and Cielo Balance issues, I was instructed to remove myself from the process altogether.

3. Project Removal: When I attempted to follow up on the Wi-Fi, Eagle Eye, and Firewall Projects, Glenn told me that he was directly managing these projects and had assigned the work to be completed by OSI.

4. IT Racks: Glenn agreed that every rack in every club needs to be redone starting in May to address compliance failures, ungrounded electrical, improper mounting, and other critical issues, in addition to the lesser matters that had been negatively impacting our technology investment. Glenn told me he was directly managing this project and had assigned the work to be completed by OSI.

5. Wi-Fi: Glenn agreed that we needed to verify that the Wi-Fi Access Points had been installed where Cerdant had identified they needed to be placed to provide the intended coverage and performance. Glenn told me this would be taken care of and that I was not to be involved.

6. M365 Licensing: After presenting the benefits from an analysis of M365 direct billing and license optimization, Glenn assigned Ryan Brooks to handle the cleanup, new billing setup, and migration to new license assignments. Some of the work was completed.

7. Adobe Sign Integration: Ryan Brooks disregarded my request for a risk/reward assessment on Adobe Sign Integration under Glenn's instruction.

Since May 8th:

- Microsoft Recommendations: When I instructed Ryan Brooks to follow Microsoft's recommendations for our Azure-hosted servers and databases, Glenn countered with an alternative, non-standard approach

Exhibit 24E-2

from Gross Mendelson. When this failed, I organized the necessary resources to implement Microsoft's recommendations, and in response, Glenn said that he was no longer interested in resolving these issues.

- Task Assignments and Information Requests: Despite repeated requests for information on Ryan Brooks' tasks and urgent priorities, I have not received the promised details, which are critical for maintaining our PCI Compliance.

During Glenn's management of the IT Department, a misleading narrative has been created, affecting others' perceptions and negatively impacting my professional reputation. I have continuously advocated for compliance with FMLA regulations and challenged the legality of applying different policies to my leave. Despite this, I have faced impediments in performing my duties and maintaining professional standards.

Several examples illustrate the issues faced:

- Cybersecurity Queries: Directing cybersecurity questions to the company president, bypassing the IT department, is highly irregular.

- Communication Restrictions: Requiring prior approval to contact anyone outside IT hampers departmental functionality.

- HR Complaints and Vendor Discrepancies: Formal HR complaints have been mishandled, and significant vendor payment discrepancies remain uninvestigated.

- Unrealistic Budget Challenges: Despite presenting precise, invoice-based data that aligns with other groups, my data-driven budget analyses have been consistently challenged without basis.

Given these ongoing issues, I have requested a third-party investigation, legal advice, PCI compliance consultation, and expert assistance in Azure technology. We have made progress by consulting with Geoff, who confirmed my previous statements about PCI compliance.

I request a follow-up on my previous request to engage Finchloom, a Microsoft-recommended expert, to address our need for qualified M365/Azure resources. This step is crucial to resolving the problems without requiring me to return to the unsustainable workload of 120-140+ hours per week.

Thank you for your attention to this urgent matter.

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

Exhibit 24E-2

OHANA
Growth Partners

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093

www.planetfitness.com

“Culture eats strategy for breakfast”

From: Ryan Wagner <Ryan.Wagner@ohanagp.com>
Sent: Tuesday, May 28, 2024 11:56 AM
To: Glenn Norris <glenn@ohanagp.com>; Justin Drummond <Justin.Drummond@ohanagp.com>
Cc: Rich Hartman <Rich.Hartman@ohanagp.com>; Karen Debus <karen.debus@ohanagp.com>; Stacey Wittelsberger (ESC) <srector@exeterstreetcapital.com>; C. Victor Brick <Victor@ohanagp.com>; Lynne Brick B.S.N. M.A. <lynne@ohanagp.com>; Terry Woods (Planet Fitness) <Terry.Woods@ohanagp.com>; Earl Ihle <Earl.Ihle@ohanagp.com>
Subject: Finchloom Flight Program

@Glenn Norris @Justin Drummond As you may recall, the plan was to replace Baltimore Consulting in 2024 due to performance issues.

The most recent issue stemmed from Matt Norris, who viewed Ryan Brooks as an unreliable resource. Matt articulated concerns about the execution of prior requests being unsatisfactory, such as the intranet project. He noted missed deadlines, which raised concerns about the impact on the speed of implementing invoice automation. This led to the decision to choose a more costly solution and agree to replace Ryan Brooks and Baltimore Consulting in 2024.

In August 2023, Finchloom was recommended to us by Microsoft and confirmed as a good option through a professional connection of mine at Microsoft. In September 2023, Ryan Brooks informed me he would not be available for the selected weekend for the emergency cloud migration, stating he did not believe we would be ready in time and did not need to notify me sooner of the timing conflict. Additionally, no one else from Baltimore Consulting was available. Glenn Norris and I immediately had a phone call and decided to engage Finchloom to see if they would be available to perform the tasks assigned to Ryan Brooks. A few days later, Ryan Brooks changed his mind and said he would be available that weekend, but he did not inform me until Sunday night during the maintenance that he doubted we would complete the migration. Ryan Brooks said he did not want to do double work, so he had neglected several key parts of his assignment, promising to complete them before 8 AM. However, these items were not completed until Wednesday.

Fast forward to March 5, 2024, Glenn Norris authorized me to reopen the RFP with Finchloom to replace Baltimore Consulting. On March 20, 2024, we had a Master Service Agreement and Flight Agreement Statement of Work, which we discussed on March 21, with a follow-up email providing these documents to Glenn Norris for review. On March 27, I followed up with Glenn Norris, who requested that I resend them. I was then away for my wedding and PFIFC created additional delays. The next follow-up was on May 8, when Glenn Norris said the documents had not been read and requested a resend. On May 10, Finchloom shared several additional resources on the program and potential references to facilitate answers to Glenn Norris' questions from our prior meeting. However, the meeting scheduled for May 13 to present this additional information was not held. Instead, Glenn Norris requested an email reply on the same day, and I provided answers to the questions and additional resources for Glenn Norris to review.

The additional information included two attachments and the following links:

Exhibit 24E-2

- Finchloom Brochure with FLIGHT and References: https://finchloom.com/wp-content/uploads/2023/12/finchloom-brochure-2024.pdf
- Finchloom FLIGHT webpage: FLIGHT | Finchloom
- FLIGHT Service listed in Microsoft Marketplace: FLIGHT Professional Services: 1-Month Implementation – Microsoft AppSource
- Flight Program Page: (Magic Program | Finchloom

Finchloom also mentioned they are prepared to schedule a meeting with a few current clients enrolled in their Flight Program.

I do not believe we have time to fully vet, hire, and onboard qualified applicants, as this process could take several months to find a singular person with the necessary skills. Finchloom's team includes many individuals with different levels of expertise and qualifications, accommodating a broad range of needs for the Flight Program. This makes them uniquely qualified to be onboarded immediately. The Flight Plan can be tailored to our budget, eliminating the need for a lengthy budget conversation. They were recommended by Microsoft, and we can easily verify the customer experience, which Finchloom is willing to expedite.

I have pre-emptively asked Finchloom to provide a minimum price and a pre-flight option with prioritized recommendations. The intention is that this month-to-month term serves as a temporary measure to demonstrate their value, leading to a fully signed Flight Program once validated.

Is there any reason not to have a call with Finchloom this week to review and, hopefully, onboard them before the end of next week?

This message may include text created with the help of natural language processing.

Book time to meet with me

Ryan Wagner
Vice President of IT
Ohana Growth Partners, LLC

OHANA
Growth Partners

office 410-252-8058 x109
212 W. Padonia Rd
Timonium, MD 21093
www.planetfitness.com

“Culture eats strategy for breakfast”